Master Photonics for Security Reliability and Safety (PSRS)

Investigation of dielectric and morphological properties of HfO_2 based ternary composite thin film deposited by CBVD for Physical unclonable functions (PUF) applications

Master Thesis Report

Presented by:

Navaneeth Tejasvi Mysore Nagendra

And defended at the

University Jean Monnet

31st August 2022

Academic Supervisor: **Dr Nathalie Destouches**

Host Supervisors: **Dr Rashmi Rani, Dr Giacomo Benvenuti**

Jury Committee:

Dr Nathalie Destouches

Dr Carlo Ricciardi

Acknowledgement

I wish to express my sincere gratitude to my supervisor, Giacomo Benvenuti for giving the opportunity to work in his structure, 3D-Oxides. I want to thank him for being a fine mentor who guided, supported, and tutored me in every stage of the internship.

Then, I thank my co-supervisor Rashmi rani for being a supportive guide who helped me to understand the new concepts while working in a company, providing advices that helped me to well understand the concepts. I thank her for always being there to discuss the unfamiliar topics which helped me to work with my full potential.

I thank equally William Maudez, who was always available for guiding me during my project and explaining me anything that I would have not fully understood regarding the manufacturing methods.

I also thank Benjamin Malthiery, for providing the technical, and academical support to understand the concepts of PUF and guid me well with many ideas that I had encountered.

I want to thank Acha Safir for giving me with information on the area and for always being available to help me with anything I needed outside the scientific sphere.

I acknowledge Estelle Wagner for the phone call we had, and providing insights for the project.

And overall, I want to thank them all, equally, for their cheerfulness and warm welcome.

Abstract

Material characteristic is a crucial part for industrial application, innovation in thin-film oxides over the period of time has drastically shifted the micro-electronics industries. The scope of this thesis is to understand HfO_2 based ternary system of $Al_2O_3/HfO_2/ZrO_2$ for possible Physical unclonable functions (PUF) applications. PUFs are cryptographic primitives used to create real and intrinsic randomness, which is essential for cryptographic and secure applications. As a result, the PUF output (response) includes characteristics that can be used to create a true random number generator (TRNG) for security applications. The most widely used PUF architectures are based on transistors and concentrate on taking advantage of the unpredictable process variances in traditional CMOS manufacturing technologies. But recent development of simple stack memristor PUFs encourages to experiment with potential thin-film materials for this regard. Understanding the randomness of thin-film that are unique to manufacturing methods are essential.

Simple structure of metal-insulator-metal (MIM) was developed using affordable ternary systems of $Al_2O_3/HfO_2/ZrO_2$ which was deposited on two different bottom electrode material of TiN and $TiO_2:Nb$. These two systems were extensively studied in order to understand the variation in electrical properties like capacitance, resistance, impedance, and dissipation losses. composition study and surface quality of these two systems were studied using SEM imaging and composition analysis techniques. Study of these systems under varying temperature and in glovebox was carried on to understand the variation in material properties. IV characterisation of the samples with cycle-to cycle (C2C) variations were studied. Based on the variation of certain properties like capacitance, and resistance, option of coating PUFs and memristor PUFs were proposed.

Extended part of the thesis also includes some numerical modelling of miniaturized optical PUFs setup using Zemax to understand the irradiance variation with patterned thin-film and divergence study of the light source.

List of figures

List of tables

Table of Contents

Investigation of dielectric and morphological properties of HfO_2 based ternary composite thin film deposited by CBVD for PUF applications

1. Introduction

1.1. Security needs

In the modern age of Internet of Things (IoT) there is drastic growth in electronics, and numerous privacy and security risks arise because of this. Some defences against these issues are provided by classical cryptography, but they all hinge on the idea of a hidden binary key: the gadgets are thought to be capable of permanently storing a piece of digital data that is and will always remain unknown to the opponent. Unfortunately, it can be very challenging to uphold this criterion. Key exposure and security breaches can result from physical attacks like invasive, semi-invasive, or side-channel attacks as well as software attacks like malware and API attacks [1]. The fact that the used devices should ideally be small, inexpensive, and resource-constrained in some business applications adds further complexity. To solve this prevalent issue in cyberspace, knowing with whom one is engaging or how to properly transmit information from the physical to the digital worlds is important, new solution built on a foundation of trust are required.

In addition to security and privacy issue, increased trend in the practice of e-commerce and asset transfer leads to greater diversity of products, but it also opens distribution channels over which manufacturers may have less control. In this situation, it becomes sense to worry that the number of fake goods would rise even more. According to a survey study by Khalil [2], the act of counterfeiting is divided into several categories, including simple copies, counterfeits made using reverse engineering, excess production from subcontractors, and parts that have been rejected during quality control operations. This threat has cost the American industrial sector an estimated US $200 billion over the past 20 years, which resulted in loss of very large number of jobs [3]. Additionally, as the International Chamber of Commerce noted in 2016 [4], trade in counterfeit goods has grown by 80% over the last five years, from US $250 billion in 2008 to more than US $461 billion in 2013. Projection in total international trade in counterfeit and pirated goods for 2022 is of US $991 Billion and this calls for some strong countermeasures.

In addition to harming the economy, it may also pose a health risk. In 2006 [5], the World Health Organization reported that 10% of medical items worldwide are fakes. The wellbeing of both individuals and entire populations is at peril because of these fake goods. In these medications, the active ingredients may be absent, diluted, or replaced with other compounds or placebos. In this instance, the dosage is not appropriate to treat the patient and poses a danger that the disease's underlying cause will become increasingly resistant to therapy.

As described in the white paper of Clemessy, the Eiffage Énergie Systèmes brand devoted to industry [6], the continuous adoption of new sensors and communication

systems in the sphere of industrial and technological systems should also be taken into account. The distinction between information systems and industrial systems is indeed fading as we move toward Industry 4.0. When these specifications were created, security was not yet a crucial component. Instead, the goal was to focus on the interoperability and durability of industrial systems. One of the biggest hazards associated with the Industrial Internet of Things (IIoT) is consequently cybersecurity. Given the variety of environments that these systems control (supply chain, warehouses, building security and energy management, transport infrastructure, hospitals, etc.), the extent of a cyber-consequences attacks are crucial. These include personal safety, property damage, environmental pollution, financial losses due to production interruptions, data theft or modification, and harm to a company's reputation. In this environment, 66% of businesses reported cyber-security incidents in 2017, and in more than one in two of those situations, the cost exceeded US $500k [7].

The quality of the components used in the construction of military equipment [8] or essential facilities like water, hospitals, gas pipelines, the energy grid, etc. must be ensured, and counterfeiting poses a latent risk to national security. Consumer applications, such as the Mirai attack (malware that transforms connected devices into bots that are then used for distributed denial of service attacks), and particularly industrial systems that oversee key services already have substantial economic and societal repercussions. The industrial programmable logic controllers (PLCs) used in Iranian power stations and drinking water distribution networks were the target of the Stuxnet worm [9], which was detected in 2010. Another prominent example is the 2015 attack on the electricity network in Ukraine [10]. Therefore, there is a very real and growing demand for anti-counterfeiting solutions to protect users online, as current cybersecurity and anti-counterfeiting technologies are unable to adequately address this issue and halt its growth. According to a report by IoT Analytics [11], authentication continues to be the weakest link in IoT security, followed by access control and data encryption.

A comprehensive solution that ensures the reliability of the authentication and the security of the transmitted data is required to create a cyber-trust environment. A product called e-tag, created by 3D-Oxides, is frequently used in conjunction with a blockchain architecture. This report is an attempt to find thin-film materials for designing electrical PUFs by studying and characterizing the materials for their electrical and morphological properties. The focus of the article is to find suitable properties that can be used to create PUF for lightweight cryptographic randomness using oxide thin-films developed by 3D-Oxides. In an extended part, to also carry some optical simulations using Zemax OpticStudio on existing optical PUF system designed by 3D-Oxides.

1.2. PUF: a comprehensive solution

Given the need for a higher security level that satisfies the modern constrain associated with the embedded system: low computational needs, cost efficiency, and limited areas are prioritized without sacrificing compatibility with cryptographic applications. In the area of cybersecurity, they stand for cutting-edge solutions [12]. Their main concept is to take use of the "random physical disorder" or "manufacturing variations" [13] that are present on small length scales in practically all physical systems. The illustrated disorder is often impossible to completely control during system creation and cannot be purposefully refabricated, not even by the original maker. It acts as distinct fingerprint [14] of each system and are 'unclonable'. A PUF, more specifically is a physical disordered system which are challenged using external stimuli or 'challenges' (C_i). When we input such challenges to the PUF we get corresponding responses (R_i) for our output. A PUF's response is based on a sophisticated physical mechanism that is exclusive to that PUF. If the same task is presented to multiple PUFs with the same design, the results will vary as seen in figure. 1. The tuple of (C_i, R_i) is known as challenge-response pairs (CRP).

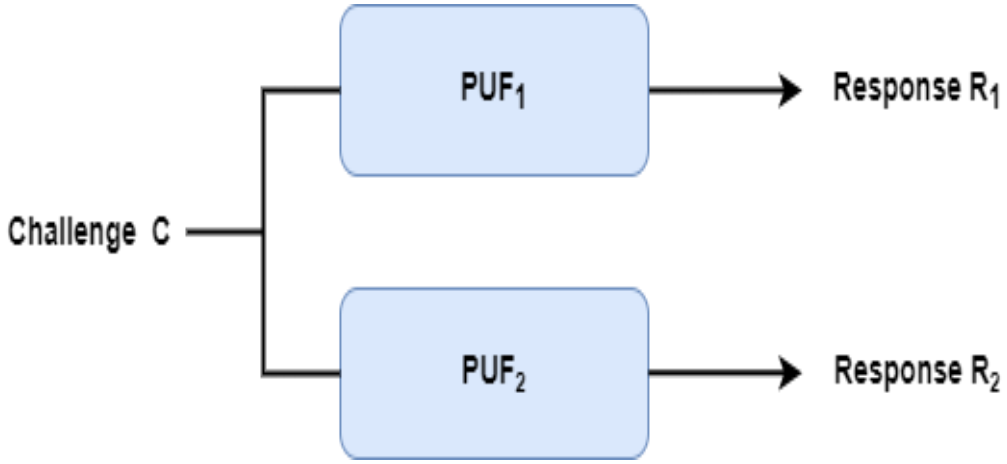


Figure 1. Schematic of uniqueness of PUF for same challenge with different responses.

Some of the commonly used PUFs are CMOS-based such as Arbiter PUR (APUF) [14], Ring Oscillator PUF (ROPUF) [15], Static Random Access Memory PUF (SRAM-PUF) [16]. Uncontrollable product variation during the fabrication of CMOS provides them with unique signature from one chip to another [17]. These chip specific signature creates delay differences on symmetrical electrical paths on a chip. This randomness in the delay produces unique PUF response for each chip [18]. Bits of information can be generated from such variation thus can be utilised in various security applications such as Key authentication [19], RFID tags [20], IP protections [21], IC piracy [22], unique identifiers and random generators [13].

PUFs are most commonly used for two purposes: secure key creation and authentication. The PUFs are often divided into "strong PUFs" and "weak PUFs" based on these two purposes. While weak PUFs are better suited for key creation, strong PUFs can be used for authentication. Based on the number of CRPs generated by the system they can be stated as, strong PUFs having large CRPs and weak PUFs with very few CRPs [23].

The restricted number of CRPs, model building assaults, reliability deterioration, and less usage area are all issues that this study solves by taking advantage of the special characteristics of nanoelectronics rather than CMOS technology. More crucially, establishing security-critical characteristics including uniqueness, homogeneity, irreversibility, and low cost [24]. Memristor PUFs have demonstrated greater resistance to assaults like reverse engineering [25] due to the inherent randomness at both the memristor level caused by the device's variation in fabrication process level, such as the cross-sectional area and variances. The user will not be able to regulate its resistance due to the fact that the generated features are not the same, allowing for the extraction of unique keys [26]. This report explores such property of material that can be used in order to create unique keys, in extended part of the project numerical simulations were carried to mimic and understand optical PUF behaviour that is designed by 3D-Oxides.

1.3. 3D-Oxides

The research organization which was established in the year 2009 with a vision and purpose to develop innovative and eco-sustainable thin film materials for diverse application in the fields of optics, photonics, electronics, and biotechnologies. The company is in Saint-Genis-Pouilly near Franco-Swiss border amidst the scientific basin created by one of the largest and most renowned facility (figure 2), the CERN (European Organization for Nuclear Research). Some of the other prominent scientific organization nearby includes the University de Genève, the Institut des Nanotechnologies de Lyon (INL), the CEA (Leti and Liten) and the Institut Néel, both in Grenoble, and the Ecole Polytechnique Fédérale de Lausanne (EPFL).

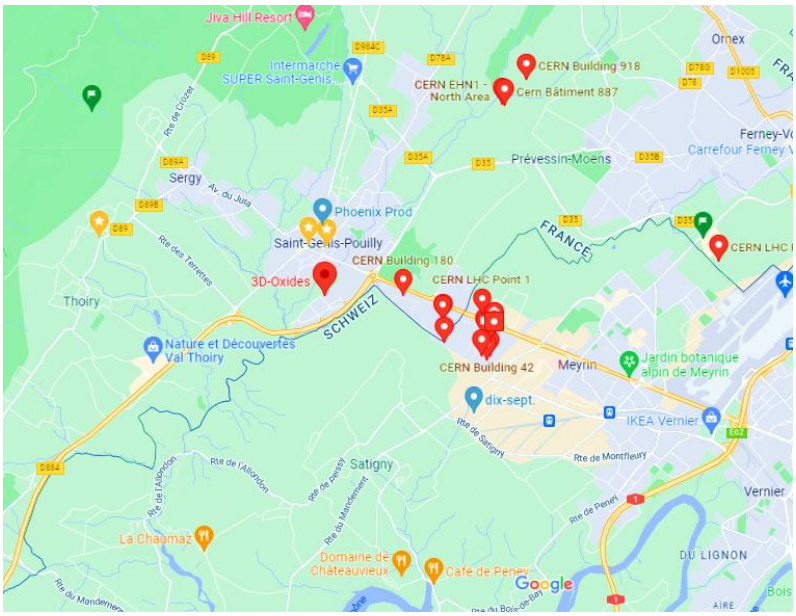


Figure 2.. Map illustrating the location of 3D-Oxides in the scientific basin of CERN

The company is active in several stages of the production chain for thin film growth, starting with the synthesis of chemical precursors and moving through process development for CBVD (Chemical Beam Vapour Deposition) systems, material science engineering, and up to the development of first device designs.

The Sybilla thin film growth equipment series, which is used to carry out CBVD processes, is likewise distinctive and the result of extensive conception work between **ABCD technologies** and **Socrate Industrie**. It has reached remarkable maturity level and performances for R&D, but still need increased maturation for production. The key main features of Sybilla equipment are its ability to produce very controlled thin films with chemical and thickness uniformity (1%) of multi-element materials even on large substrates (450 mm) or controlled gradients providing powerful combinatorial approach as well as its ability to produce complex nanostructures utilizing a single-step bottom-up additive growth process with stencil masks or laser-assisted growth

1.4. CBVD Technique: Innovative approach to produce PUF

Main part of the research is to explore the dielectric and morphological characteristics of ternary-based material of $Al_2O_3/HfO_2/ZrO_2$ on two different bottom electrodes of TiN and $TiO_2:Nb$ for PUF applications. These thin-films were deposited using patented in-house technique that is unique to 3D-Oxides called Chemical Beam Vapour Deposition (CBVD) [27, 28, 29].

There are several synthesis routes that can be used to create thin films, ranging from Shake 'n bake methods (solid state reactions) by tape casting to a softer approach, the Chimie Douce method using sol-gel reactions. Moving on to gas-phase deposition techniques like Physical Vapour Deposition (PVD) [30], Chemical Vapour Deposition (CVD) [31], or Atomic Layer Deposition (ALD) [32], whether technological or economical, each have their own advantages and disadvantages. Beyond these issues, the manufacturing method of choice has a significant impact on the final qualities of the films. The process does, in fact this have an effect on the structure at both the atomic and microscopic levels.

The CBVD process is a hybrid technique that combines the well-known molecular beam epitaxy (MBE) and chemical vapour deposition processes [33]. In this process, the precursors are transported to the substrate in gas phase. Absence of interactions in the precursor beam, and cryo-panels are used to preserve the beam's quality and high vacuum [34]. Additionally, the use of Knudsen cells offers a tightly controlled supply of the precursors in the gas phase (by maintaining a consistent cell temperature, in accordance with the Clapeyron relation [35, 36]), whose direction follows a line-of-sight trajectory [27, 35-37]. In order to simulate the film growth prior to deposition [27, 29], the distribution of the precursor impingements on the substrate follows a cosine law. This method opens up a wide range of possibilities for the synthesis of ternary oxides by allowing the simultaneous deposition of three separate precursors through six different pre-chambers, figure 3.

Both kinetic and thermodynamic laws govern this process. However, kinetic laws appear to be more significant because they determine how a film grows [33, 38]. Deposition should take place in the mass transport limited regime, or when the delivery of precursors to the substrate is the rate determining step (RDS) of the film growth, in order to optimize the control of the growth rate. This regime can be operated at modest precursor flow rates; however, when substrate temperature rises, precursor flow rates can also rise [27, 38]. These two variables are very important since they control the atoms and microstructures and, as a result, the physicochemical characteristics of the formed film. Precursor selection [39] and operating setup are further crucial elements of the CBVD process (i.e., which of the 18 cells are used [27]). Following the flow simulations as shown on figure 4, the set-up used makes it possible to develop films with regulated chemical composition or thickness gradients. As seen the depositions vary depending on the flow ratio and the activated cell count.

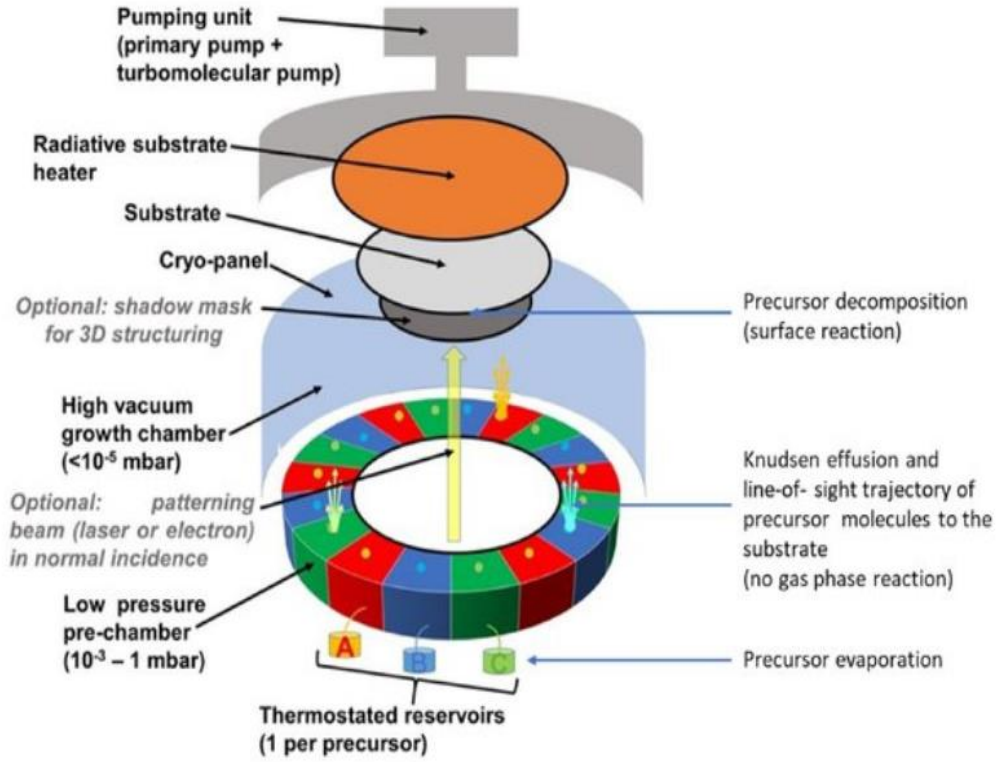


Figure 3. Schematic of CBVD deposition chamber of Sybilla equipment showing different precursor channels.

The film qualities can be evaluated using a variety of characterization approaches, either in-situ to provide dynamic measurement or ex-situ to analyse the physicochemical properties of the film, such as resistivity measurements. In terms of applications, performing combinatorial research of surface coating with binary or ternary oxides appears to be one of, if not the best uses for CBVD equipment. Furthermore, the use of a stencil mask eliminates the need to first develop a film and then pattern it using a top-down technique [40], enabling the growth of patterned thin films in a simple and single bottom-up phase. The CBVD method is thus a clever and extremely sophisticated instrument with immense potential for creating complex thin film architectures, given that all of the operating parameters are thoroughly understood, both individually and collectively, as their synergy is crucial.

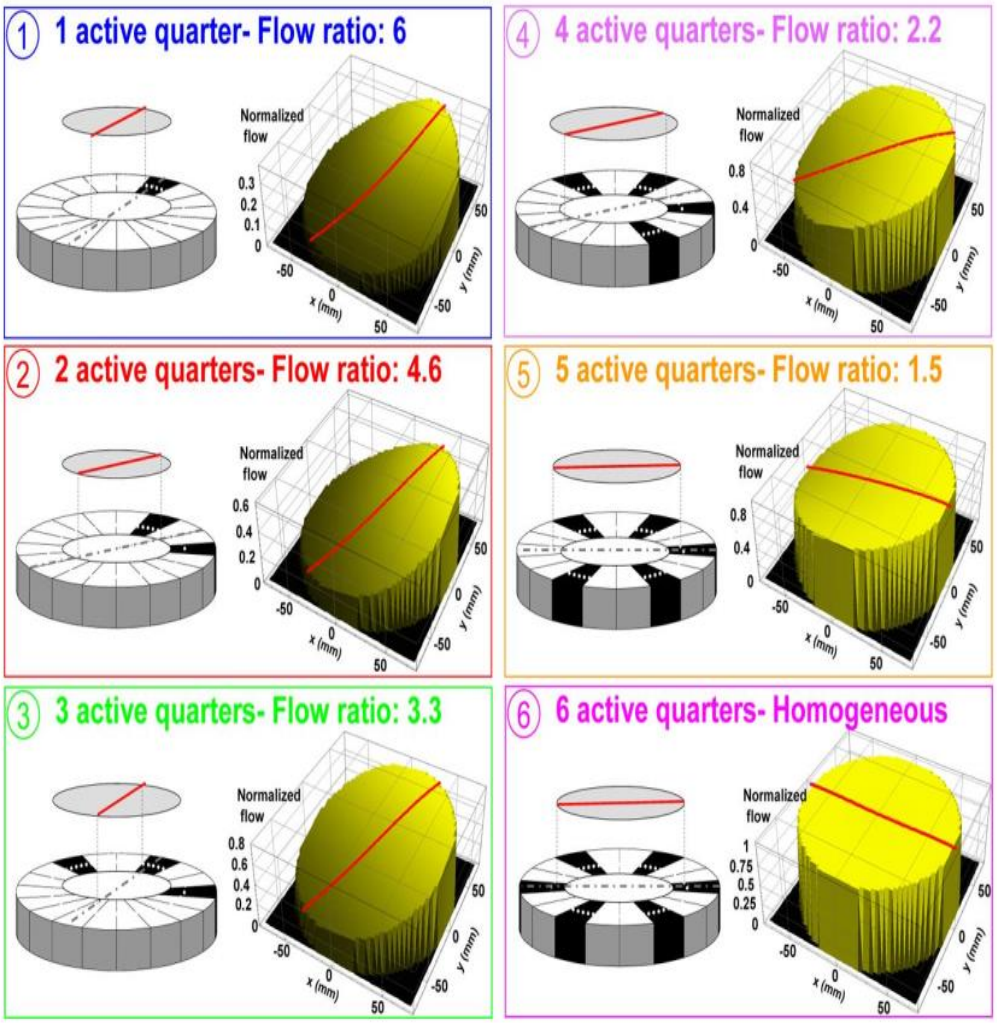


Figure 4. The different gradients achievable according to the configuration used [27]

Liberty to produce 3D thin films with unique material properties on every deposition stage gives added advantageous for this technique to use it for PUF applications. In addition to manufacturing randomness, use of cleaver design and combinatorial approach one can use CBVD technique to produce unique materials that can be used for strong optical PUFs application (Fig.5). The quality of deposits produced by this method is consistent with simulations produced by mathematical models. If the chemical reaction is constrained by the precursors, it is possible to mimic the thin film thickness and chemical composition with accuracy this is one of the main benefits of the CBVD approach. Numerous benefits are made possible by the potential to create intricate nano 3D-patterned oxides with many different functionalities.

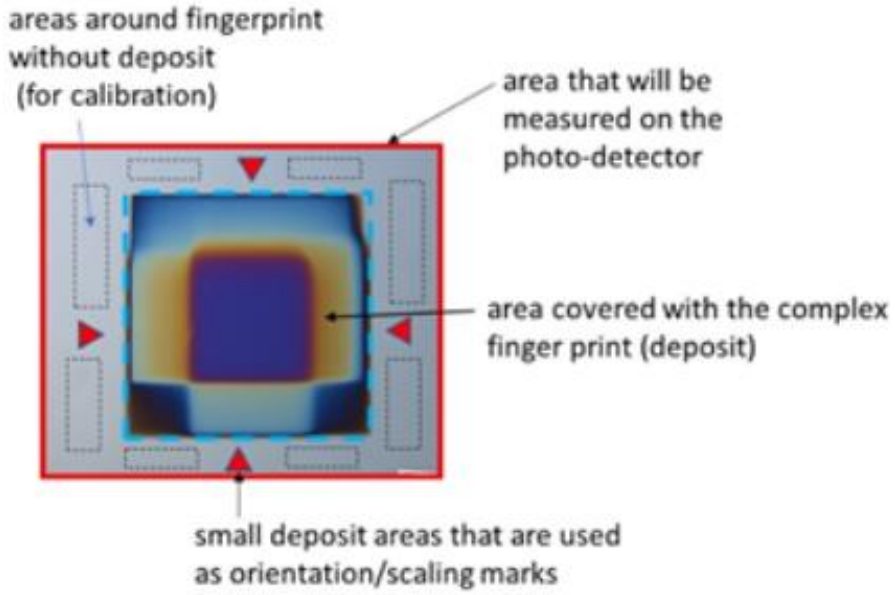


Figure 5. Thin film format for Optical PUF applications with calibrations areas and correction pattern.

On cleaver use of high-K materials such as HfO_2 combined with other oxides like ZrO_2, TiO_2, or Al_2O_3 a binary or ternary oxide thin-films can be produced in a single go and can be used for specific applications like memristors, MIM capacitors or optical holograms.

2. PUF based on electrical properties of the material

2.1 Electronic PUFs: definition and design

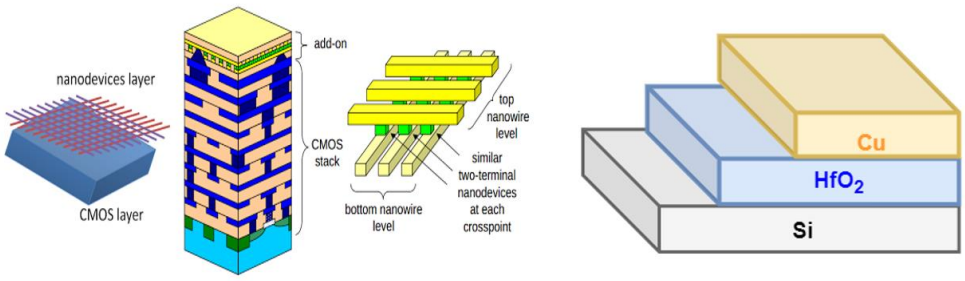
Classification of PUFs can be done based upon the evaluating parameters. If the variation in electrical parameters like capacitance, resistance or impedance etc to creates variation in evaluating parameter like frequency, time etc. Then they can be called as electronic PUF [41]. The fabrication process of the material gives unique characteristics which allows us to extract material specific keys. 3D PUFs that works on electronic properties relays majorly on CMOS technologies that consumer electronics adopted. Some of the industrial favoured PUF and their defining parameters are listed in Table 1.

Year	PUF Name	Parameter
1993	Paper PUF	Light intensity
1994	Magnetic PUF	Magnetic field intensity
2002	Optical PUF	Light intensity
2002	**Ring-oscillator PUF**	Frequency
2004	**Arbiter PUF**	Time
2006	Coating PUF	Capacitance
2007	**SRAM PUF**	Bistable state
2011	TERO PUF	Frequency
2013	**Memristor PUF**	Bistable state
2015	**Q EPUF**	Voltage – current characteristic
2017	Liquid crystal PUF	Frequency

Table 1.Table of different PUFs chronologically classified based on their properties. Industrial focus in the bold font [41]

Some of the most published articles on electronic PUFs are on Ring-oscillator PUF, Arbiter PUF, Static random-access memory (SRAM) PUF, memristor PUF, and quantum electronic (Q) PUF.

Complex electrical circuits need to be constructed to realize these electronic PUFs, in general most of these PUFs are CMOS. This is indeed an expensive and unreliable way to produce PUFs for large scale applications, this makes it necessary to design a compact and simplistic design of thin-film materials, figure 6. In addition to manufacturing complexity CMOS PUFs poses higher susceptibility to modelling attacks. In this report we explore the possibility of using unique properties of thin-film nano-electronics rather than CMOS technology to build weak PUFs .



a. 3D hybrid CMOS memristor **b. Stacked HfO_2 thin-film memristor**

Figure 6. Illustration showing the difference between a. complex CMOS memristor and, b. simple stack HfO_2 memristor.

2.2 Material electrical properties that could be measured for PUFs applications

As established in the previous section it is clear that some of the electrical properties like capacitance, resistance, or dielectric constant creates variation in frequency, time etc., this can be used to design all electronic PUFs, some of the most industrially favoured are ring-oscillator PUF, arbiter PUF, SRAM PUF, memristor PUF, coating PUF, and Q PUF [41]. It is important to understand how these PUFs operate.

Ring-oscillator PUF: when a signal passes through an oscillator circuit made of inverter/NOT logic gates, the Ring Oscillator PUF [42] measures the variation in the delay and, consequently, frequency of the signal. This is based on the manufacturing variance of the components that make up the signal line and logic gate. The oscillator consists of odd number of these gates to ensure inverted signal feedback to any input signal., thus the oscillation in the system. The system oscillates with certain frequency that is unique to the randomness in the device, this can be considered as the response.

Arbiter PUF: an arbiter PUF [43] describes a system by comparing the differences in the propagation times of two electrical signals traveling along hypothetically symmetrical routes. This is based on the manufacturing variation used to create these pathways. A signal source is connected to an arbiter component by the PUF, which is made up of many cells. Depending on which of two input signals split from the signal source reaches the arbiter component first, the component outputs a binary signal. The activation state of the switch in each cell presents a distinct issue since each switch has the ability to route both signals through a different signal line while it is in its active state. A constant "winner" signal will be linked with each "race," or guided path, as a result of the random fluctuations in the conductor and switching gates that the signal goes through. Challenges are created by the on/off nature of the routing switches (and arbiter position or numbering for several of these systems) and binary based responses on the quicker path following this switching are noted.

Memristor PUF: memristors are electrical components that, when a threshold voltage is achieved, alternate between a high and low resistance state. The memristor enters a low resistance state over a forward voltage threshold, and with a negative current, it returns to a high resistance state. Based on changes at both the manufacturing and resetting stages, this results in each memristor in an array having either a high or low resistance state, in an unpredictable but reproducible manner. The circuitry is then built around reading the resistance state that each memristor is in, turning that information into a PUF response depending on a challenge of the array's memristors number or position [44].

Coating PUF: a coating PUF [45] entails measuring the capacitance across a pair of comb-shaped sensors in an integrated circuits top layer. A dielectric coating is sprayed on top of the sensors to expressly induce significant randomization due to the variation in the coating's properties (such as thickness) over the surface of the PUF at the manufacturing stage.

Quantum electronic PUF, for unique device authentication, the Quantum Electronic PUF (Q-EPUF) [46] uses different resonant tunnelling diodes (RTDs). A quantum well is surrounded by two barriers in RTDs, and only electrons with a specific energy can tunnel from one side to the other. The voltage across the device determines the energy level of the confined quantum well in comparison to the energy level of the electrons in the emitter, and the current through the diode is equivalent to the number of electrons flowing through the system. More electrons have the particular energy needed to tunnel past the barriers through the constrained energy level in the well as the applied voltage rises from zero voltage, which causes the current to rise.

As observed, variation in capacitance, frequency, time, or resistance can be used in defining specific functional PUFs, but working with HfO_2 binary or ternary system it is much more favourable to move with memristor PUFs. It has already been exhibited that HfO_2 based thin-film nano-electrical stacks can be used as memristors

2.3 High-K dielectrics and ternary dielectrics for memristor-PUF application

In a growing age of micro-electronics and IoT there is a need to substitute Silica as a main material. It is realized that the growing demand to miniaturize metal-oxide-semiconductor (MOS) devices has proven to be very challenging as we move towards sub-nano meter size of SiO_2, in a 1~2 nm thick SiO_2 we often encounter high leakage currents that leads to reliability problems in the devices. This makes it necessary to find alternative materials that can overcome this problem. High K dielectric materials has been drawing more and more attention in these days for their properties and extended multi-functionalities. In the case of PUFs applications, achieving multi-functional materials enables to obtain more challenge typologies that can be used in parallel to both strengthen PUFs uncolorability and information density contained in the PUF.

.Hafnium dioxide (HfO_2) has emerged as one of the industrially leading choices as it has high dielectric constant (25), high band gap (5.8 eV), and high heat of formation (271K Cal/mol) that are thermally stable and are highly compatible with polysilicon gate processes [47]. If right manufacturing methods are not followed, it will result in defective HfO_2 which may cause high losses and increases number of oxide charges. For these reasons, HfO_2 is an interesting choice for PUFs application.

Compared to other techniques, Chemical Beam Vapor Deposition (CBVD) developed by 3D-Oxides has many advantages such as high deposition rate, good adhesion, uniformity and suitability for large area deposition]. Systematic studies were focused on modulations of morphologies, sizes, and crystallinity of oxide thin-films synthesized by CBVD technique.

For memristor application it has been previously demonstrated by 3D-Oxide [48] that HfO_2 thin films on selective thickness range produces best results, as thin-film thickness decreases it was observed that the leakage current was too high. This led to an experimentation with binary and ternary oxides of HfO_2 to produce much stable devices. Zr has proven to be one of the most favoured dopants that can be introduced into HfO_2 system to produce a stable memory device. The physical and chemical characteristics of ZrO_2 and HfO_2 is strikingly similar. Zr is a tetravalent element with an atomic radius (155 pm) that is nearly identical to that of Hf (155 pm) [49]. They have nearly comparable lattice constants and equivalent crystal phases. The HfO_2/ZrO_2 system generates single phase solid solution over the full composition range as a result of their similarities [50]. In the semiconductor industry, HfO_2 and ZrO_2 are highly developed materials since they are employed as standard materials for the high-k gate dielectric layer in modern capacitors for DRAM and metal-oxide-semiconductor field effect transistors (MOSFET). They make excellent memory devices with much stable working ranges, still we can minimize the leakage current by adding Al_2O_3 to this making a ternary composition using HfO_2. Al is a trivalent material which is about ~19% smaller than Hf having atomic radius of 125 pm. In recent studies it has been shown that Al doped Hf to have good ferro-electric properties when optimize [51]. This gave us the motivation to create new ternary system of $Al_2O_3/HfO_2/ZrO_2$.

The randomness source must be truly random in order to maintain the security of the cryptographic primitives; otherwise, the entire system will fail. To guarantee the security of crypto-systems, true random number generators (TRNGs) are necessary. Using TRNGs, physical phenomena' unpredictability is extracted. TRNG based on Cu/AlO_x and Ti/HfO_x memristors with non-volatile [52], the suggested memristive devices required SET- RESET pulses for each output bit and careful calibration of the applied voltage because they were non-volatile. Much robust TiO_x [53]– based devices that works with small current fluctuation were designed, but this took complicated algorithms and post processing of costly circuit to ensure the generated bits quality. $Pt/Ag/Ag{:}SiO_2/Pt$ memristors [54] without complex post processing algorithms were proposed but as one can see it is very complex and costly to manufacture. Cost-efficient PUFs made up of $Cu/HfO_{2-x}/p^{++}Si$ [26] was proposed that is both robust and easy to produce. It should also be noted that coating PUFs can also be fabricated using the uniqueness in the thin-film manufacturing variations. Previous study on memristive properties of HfO_2 [48] was conducted in 3D-Oxides.

To minimize the losses and to have a much stable system, HfO_2 based ternary system was proposed. Thin-film ternary system of $Al_2O_3/HfO_2/ZrO_2$ was produced using affordable oxides and single stage manufacturing techniques. Two different bottom electrodes of TiN and $TiO_2{:}Nb$ were tested. the top electrode of Ag can be further replaced by affordable materials like Cu in future. The bottom electrode can also play a significant role in maintaining cost and tight budgets. So in-house deposition of $TiO_2{:}Nb$ as bottom electrode was carried on and characterized to know the difference. Understanding variation such as capacitance, resistance or impedance in these films can help us to fabricate specific PUFs.

3. PUF based on optical properties of the material

3.1 Optical PUF: definition and design

This group of PUFs measures an object's implicit randomness using light that has been emitted. The evaluation system provides the light that is reflected, either as a laser in a paper PUF [41] or as directed light in a CD PUF [41]. Electronic PUFs are often vulnerable to numerical modelling attacks and doesn't offer much entropy. This demands strong PUFs like optical PUFs that has higher (C_i, R_i) pairs to work with. 3D-Oxides developed thin-film with manufacturing variations that are unique to its fabrication method of CBVD. The optical thickness and refractive index of the internal thin layer cause the emergence of the iridescence phenomena. The device on which the film is applied is characterized using an optical reading method.

3D-Oxides is working on a concept of PUF that uses transmittance of light to extract uniqueness of thin-film. Based on the variation in the film, such as thickness over the region of PUF one can expect to create very strong PUFs. The setup is something similar to what is illustrated in figure 7, a light emitter of our choice, unique optical token, and a detector.

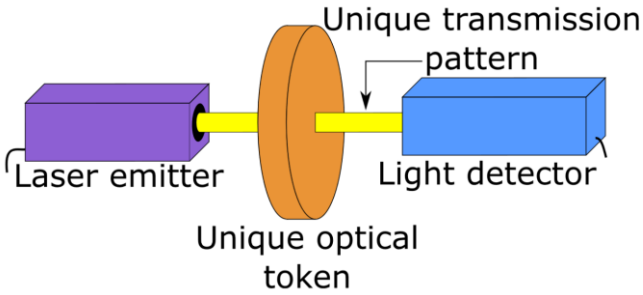


Figure 7. Illustration of the explicit setup of possible optical PUF design to extract uniqueness in the system.

3.2 TiO_2 based PUF integrated on a chip investigation

TiO_2 thin-films developed by 3D-Oxides have proven to have manufacturing variation that are unique to each single sample with regards to the transmittance pattern of

the PUF. A first PoC (Proof of Concept) has been carried out at macro-scale using a full wafer with a TiO_2 gradient and macro light sources (LEDs) and sensors. The purpose of the present work has been related to miniaturization of this first PoC and to introduce/manage eventual interference effects appearing with miniaturization between two adjacent dots leading to cross-talk. Optical modelling of the PUF has been done to understand the light behaviour in the material with Zemax software.

3.3 Numerical simulation approach – Zemax software

Zemax is one of the many simulations software that are in market like OSLO, CODE V. It has relatively easy user interface to deal with the simulations and design, this is the reason why many optical engineers and designers prefer Zemax over other software.

Optical engineers can now quickly simulate the performance of very sophisticated system using ray tracing tools like ZEMAX or CODE V. Small ray angles and heights are used in paraxial ray tracing. Compared to the manual ray tracing of light the modern computing software make the job easy and efficient [55].

The main objectives of using optical designing software was to model a miniaturize optical PUF and to conduct ray tracing to understand possible light propagation through patterned thin-film and to visualize irradiance differences at different illumination positions.

4. Experiment and analysis

The investigation of a material's dipole or ion mobility is known as a dielectric analysis. By applying an alternating current (AC) voltage to the sample and recording the current, one can determine the mobility of these charged groups. Two dielectric qualities, capacitance, or the material's capacity to store charges, and conductance, or the mobility of charged carriers inside the material, which can be connected to the observed impedance.

By measuring a material's dielectric properties, one can learn more about its physical and chemical structural properties as well as process behaviour. In a material, dipoles will try to align themselves with the applied electrical field, whereas ions will move in towards the electrodes with the opposite polarity.

Changes in the mobility of ions correlate to the material viscosity and reaction kinetics of developing systems, whereas variations in the degree of alignment of dipoles as a function of temperature and frequency provide information about physical transitions. These changes can be measured and can be used for PUF application. Selective primary and secondary parameter of the material are measured using BK precision's 880 LCR meter (details in Annexure B). Five particular test frequencies of 100 Hz, 1 kHz, 10 kHz, and 100 kHz which can operate in series and parallel modes are used to record these parameters.

Main part of the thesis is to fabricate metal-insulator-metal (MIM) structures (figure 8) and to experiment with the variation in electrical properties of these samples due to the change in bottom electrode. And again, these samples were subjected under various frequency to further analyses the variational responses in the material. and analyse the samples that are deposited using CBVD technique.

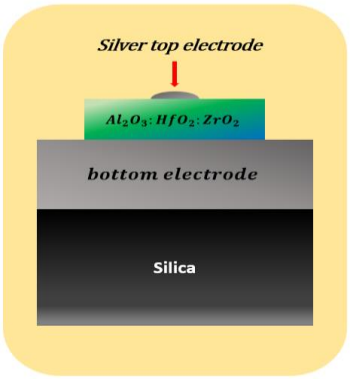


Figure 8. Schematic of thin-film metal-insulator-metal stack of the fabricated device.

Based on the selection of the bottom electrode material, two ternary materials based on HfO_2 were fabricated but they both have common silver top electrode. Stack of bottom electrode, thin-film material and top Ag electrode in cumulative can be called as system, one constructed using ternary composite are ternary system. Each of these devices further has a variation in thin-film composition, giving three distinct samples for each device. These two variations in the devices and the labelling of the samples in the wafer is illustrated in figure 9. Samples are labelled as S1, S2, S3, S4, and S5 from left to right, wafer is symmetric about the dotted line and right and left half of the wafer has similar labels.

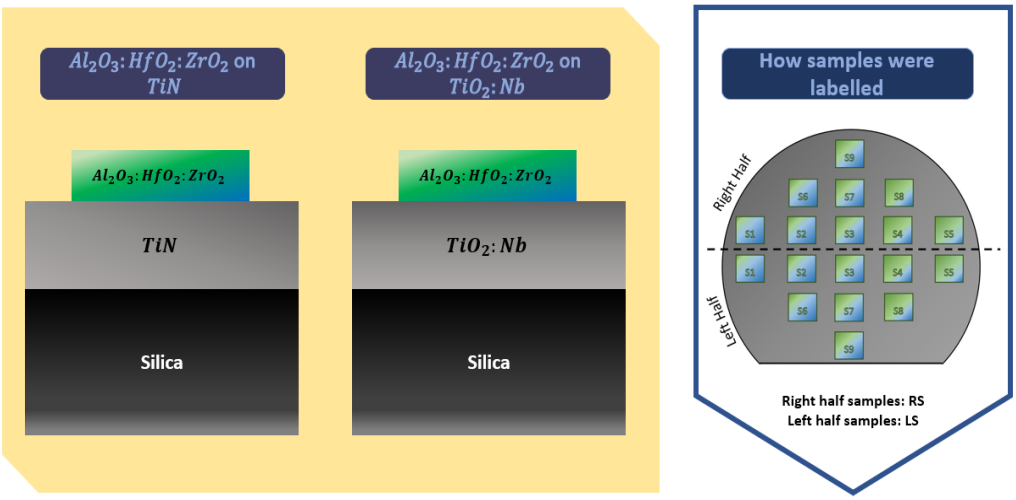


Figure 9. Schematic of variation in bottom electrode and labelling of the samples in the wafer.

4.1 Ternary system 1

For ternary system one, $Al_2O_3/HfO_2/ZrO_2$ thin-film was deposited on uniformly coated TiN on silicon wafer. The samples are deposited using masked deposition techniques to have different composition samples in a single wafer (ref. figure 10), it is to be noted that the thickness of the thin-film to be same. In order to understand the variation in the electrical responses one need to understand the composition difference, thickness variation, surface quality of such samples. Green, blue, and red dot around the edge of the sample represents the distinct flow of different precursors from different channels (ref. figure 3).

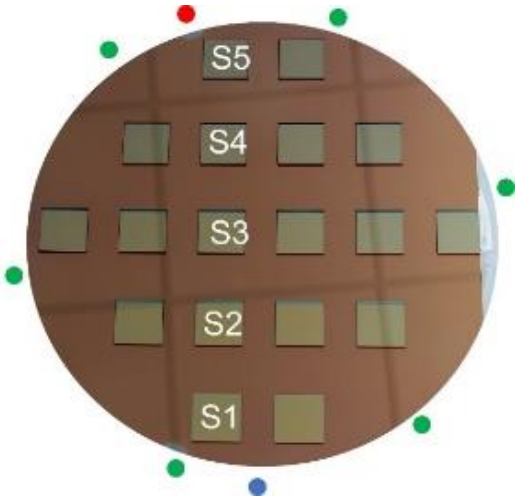


Figure 10. TiN coated silicon wafer having different composition thin-film samples deposited using CBVD technique.

4.1.1 Morphological and composition results

The morphology and composition of these samples gives us the idea of surface quality and electrical variation in the system. Hitachi's SU3800 scanning electron microscope is used to observe the surface and cross-section of these sample. EDS analysis of these samples gives us the idea of composition. Figure 11, shows the surface morphology of $Al_2O_3/HfO_2/ZrO_2$ on TiN using SEM, it shows us the granule distribution of the composition along the surface. The size of these granules was measured using advanced tools in SEM which on average was measured to be 100 nm. The distribution seems to be continuous without prominent voids and trenches, this demonstrates the superior surface quality of CBVD technique. The cross-sectional SEM image can be used to know the thickness of the thin-film, three measurements were done at three different sites of the sample and thickness was averaged at 205 nm. The measures were consistence in the value at these sites and this proves that the sample has uniformity and homogeneity of the thin-film. The TiN acts as bottom electrode which was deposited by third-party manufacturer and have uniform thickness of ~100 nm (as provided by the supplier).

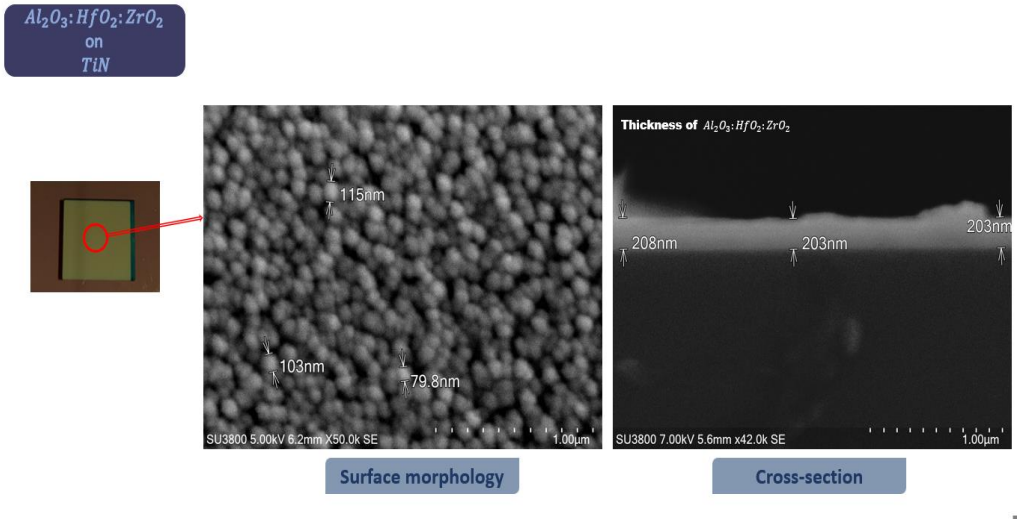


Figure 11. SEM image demonstrating granule distribution of $Al_2O_3/HfO_2/ZrO_2$ and cross-section image having thickness marking along three different points of the sample.

EDS composition analysis was carried on and the atomic percent (At %) of Al, Zr, and Hf are listed in the table 2. This allows us to select the samples of interest to filter out among many that are deposited on the wafer.

From the table 2 we can see this doesn't add up to 100 % as there are majority elements like carbon, oxygen, and silicon are excluded. Here S1 can be labelled as Zr rich, S2 can be labelled 50 – 50, and S4 to be Al rich. To our convenience they will be referred as sample 1, sample 2, and sample 3 respectively in the further part of the report.

Material: $Al_2O_3/HfO_2/ZrO_2$ on TiN			
Sample	**composition in At %**		
	Al	**Zr**	**Hf**
S1	4.1	6.9	1.3
S2	5.4	5.7	1.2
S3	6.8	3.8	1.1
S4	8.2	2.8	1.1
S5	9	1.8	1

Table 2. listing of Al, Zr, and Hf and their composition chart for different samples of the wafer of ternary system 1.

4.1.2 Dielectric characterization results

Based upon the morphological and EDS data, suitable samples were taken for dielectric characterization. Capacitance, impedance, and dielectric loss ($tan(\delta)$) were

recorded in parallel mode and resistance in series mode, this was for three samples at four different frequencies (using acquisition setup described in annexure C and D). Capacitance of the material varies vastly based upon the shape, size and material of the top electrode. In our case silver top electrode is manually placed on the top of the film which results in in-homogeneity from one sample to other. This can be corrected by using dielectric constant, as it considers silver electrode area A and dielectric layer thickness d (refer equation 1 and 2).

$$C_0 = \frac{A}{d}\epsilon_0 \quad (1)$$

Capacitance in free space C_0 can be calculated using thickness of the dielectric and area of the silver electrode, ϵ_0 is the permittivity in free space. Once C_0 is calculated, dielectric constant κ can be extracted using equation 2. Where C is the measured capacitance

$$\kappa = \frac{C}{C_0} \quad (2)$$

Variation of dielectric constant with frequency for three samples in figure 12A. one can see how dielectric constant is higher for lower frequency for all three samples. sample 1 has maximum capacitance of ~ 10 at lower frequency of 100 Hz, as we increase the frequency from 100 Hz to 100 kHz, we can see a drop in dielectric constant to ~ 9. For sample 2, dielectric constant of maximum ~ 13 at low frequency and minimum of ~ 10 at high frequency were observed, and for sample 3 it was observed to have maximum dielectric constant of ~ 16 and minimum of ~ 12. The trend of variation is same for all three samples, but sample 3 has higher dielectric constant than sample 2 which is higher than sample 1, from preliminary observations variation of $33.33\ \%, 30\ \%$, and $11.1\ \%$ for sample 3, sample 2, and sample 1 were calculated.

Dissipation loss variation with frequency in figure 12B, one can say for sample 1 we have high loss of 0.129 at lower frequency of 100 Hz and then as frequency increases, we see decrease in loss until 1 kHz, then further increase in the frequency to 100 kHz, a relatively high loss was observed. And for sample 2 and 3, one can see a similar trend but see an increasing loss for 1 kHz and 100 kHz. Variation of almost 100 - 143 % was recorded for all the samples.

Impedance variation with frequency from figure 12C, one can see a decrease in the value of impedance as frequency increases, this is common for all the samples. If sample 1 is considered, a maximum value of $2.5x10^6\ \Omega$ was recorded at 100 Hz and

minimum value of $2.8x10^3\ \Omega$ at 100 kHz. This means we see about $9x10^4$ % variation between max and min value.

Variation of resistance with frequency in the figure 12D, the trend of variation in the resistance value with frequency is similar to that of impedance. Decrease in resistance value is observed as frequency increases, this is same for all the samples. For sample 1, maximum of $5x10^5\ \Omega$ was observed at 100 Hz and minimum value of 155 Ω at 100 kHz. Similar to that of impedance we see larger variation between min and max value of the resistance.

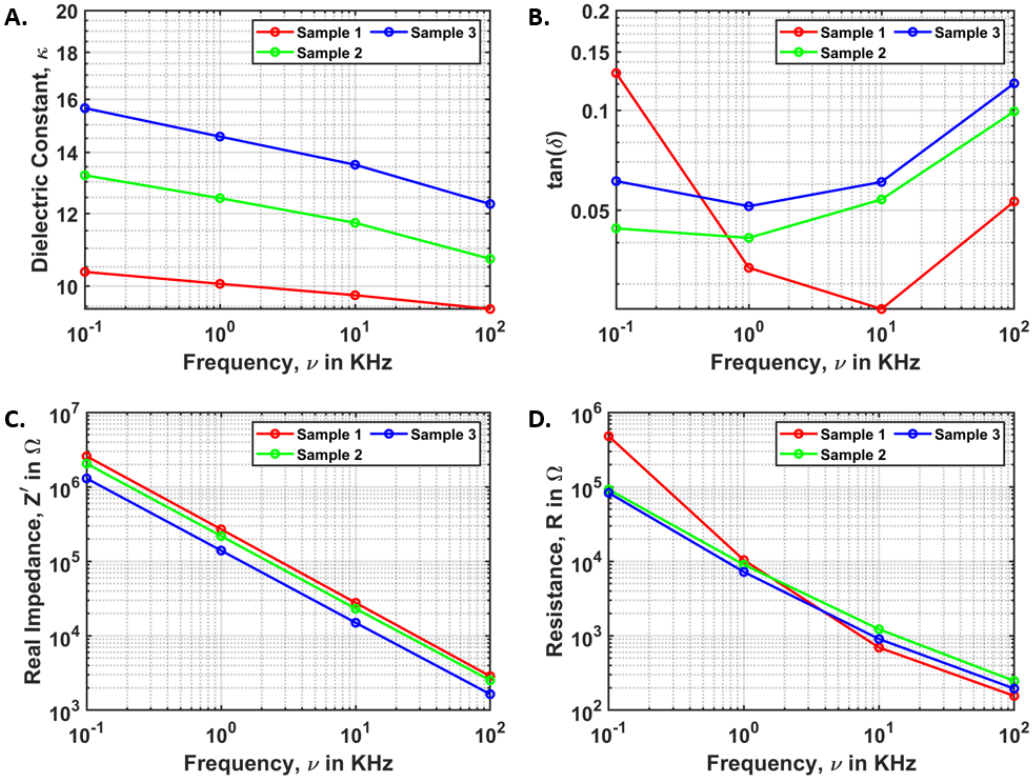


Figure 12. From A to D, we have dielectric constant, dissipation loss ($tan(\delta)$), impedance Z', and resistance and its variation with frequency for sample 1, sample 2, and sample 3.

4.1.3 Influence of external parameters

Samples were put inside a glove box that is free from oxygen and parameters were recorded using remote acquisition setup. variation in capacitance, dissipation loss, impedance, and resistance with frequency under this condition.

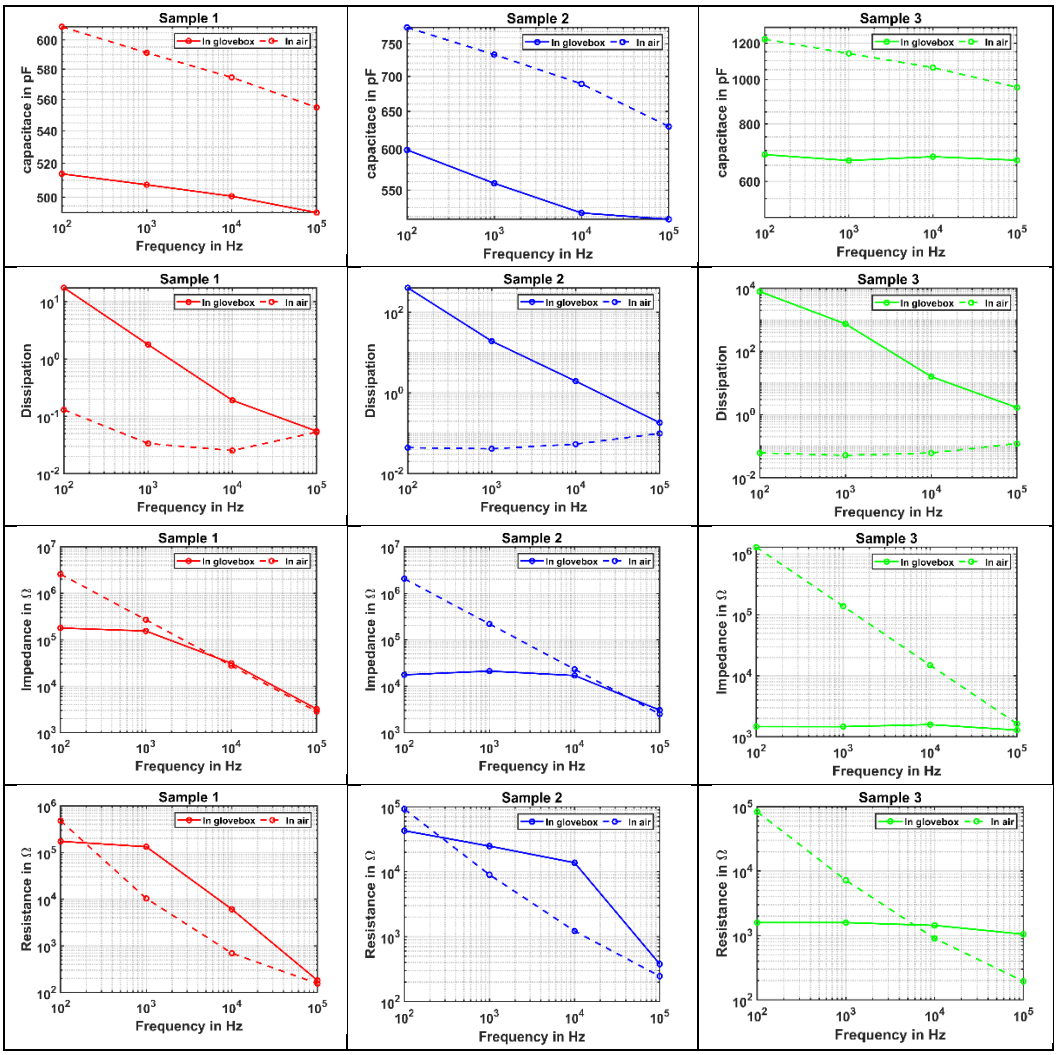


Figure 13. Variation of capacitance, dissipation loss, impedance, and resistance due to frequency for sample 1, sample 2, and sample 3 in glovebox and in open air is plotted.

It can be seen in figure 13 that the capacitance for all three samples is higher in glovebox than that of in air, a variation of about 16 % can be seen in the sample 1 and this is similar to that of sample 2, and sample 3.

Dissipation loss for the samples seems to be decreased inside a glovebox compared to sample in air. Clear variational trend cannot be drafted in regards to impedance and resistance of these sample inside the glovebox as some unexpected behaviours were observed by the samples. Impedance and resistance value seems to decrease from sample 1 to sample 2 and sample 2 to sample 3. Sample with rich Al composition tend to have very less impedance and resistance in glovebox for the whole frequency range.

4.1.4 I-V characterisation

Figure 14 shows the current – voltage (IV) curve for ternary HfO_2 system of $Al_2O_3/HfO_2/ZrO_2$ on TiN. Bias voltage ranging from $-10\ to\ +10\ V$, at 0 voltage it is expected to have 0 current and as voltage increases in positive bias the current increases much like a linear curve and as we go back to $-10\ V$ we see the similar decrease in trend, there is no prominent loop either in positive and negative bias but can be seldomly seen in all three samples. This is kind of same for sample 2, and sample 3. Maximum recorded current at higher voltage for sample 1 is around $105\ mV$, for sample 2 is around $67\ mV$, and for sample 3 it is around $122\ mV$. These are the values at positive bias, at negative bias the maximum current recorded are $-\ 95\ mV, -\ 85\ mV, and\ -\ 122\ mV$ respectively.

For sample 1 in positive bias at $10\ V$, maximum variation of 36 % increase and 16 % decrease in current to that of sample 2 and sample 3 was observed. In negative bias at $-10\ V$, we observed 14% decrease and 20% increase in current to that of sample 2 and sample 3.

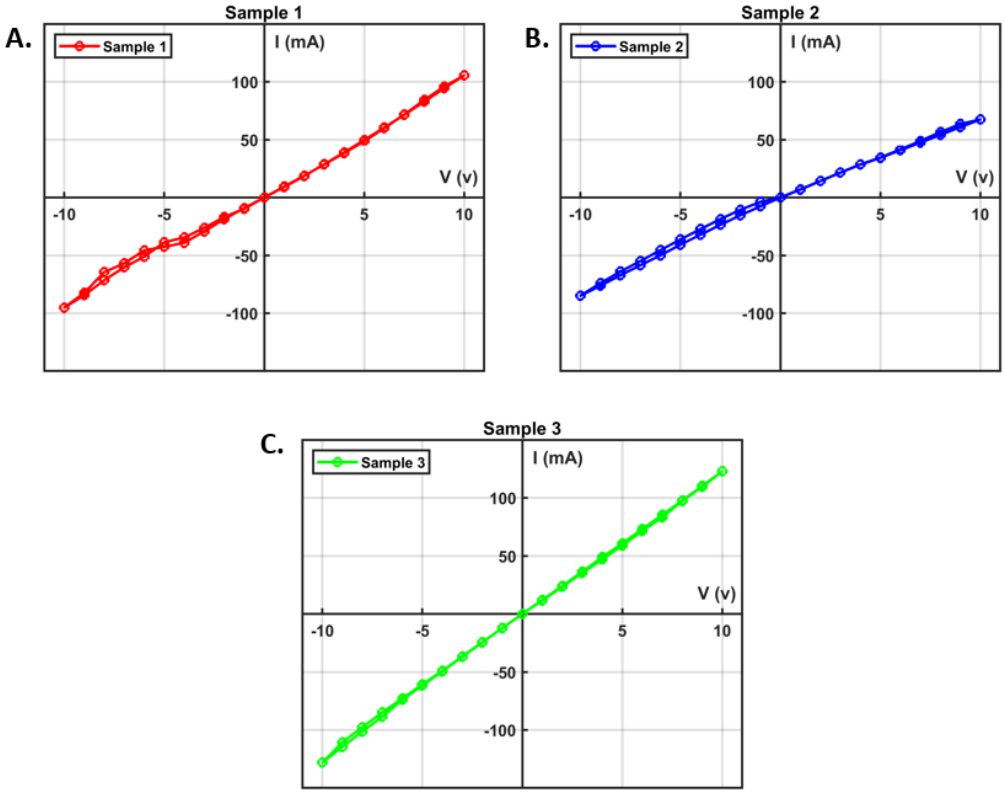


Figure 14. I-V characteristics plot for a. sample1, b. sample 2, and c. sample 3.

Further, sample 1 was tested for its Cycle-cycle (C2C) robustness by repeating the processes of acquisition continuously for four times, figure 15. This work makes use of the stochastic switching characteristic of memristor devices as an entropy source to produce random output. In addition to fabrication changes, the entropy source is inherited from the device's ionic activity, which helps with resistance switching. Based on these variables, the fingerprint IV characteristics of the memristor devices differ randomly from one device to the next and from one cycle of a memristor cell to the next. This kind of behaviour is undesired for memory application for computation and sensing, it is much favoured for hardware securities.

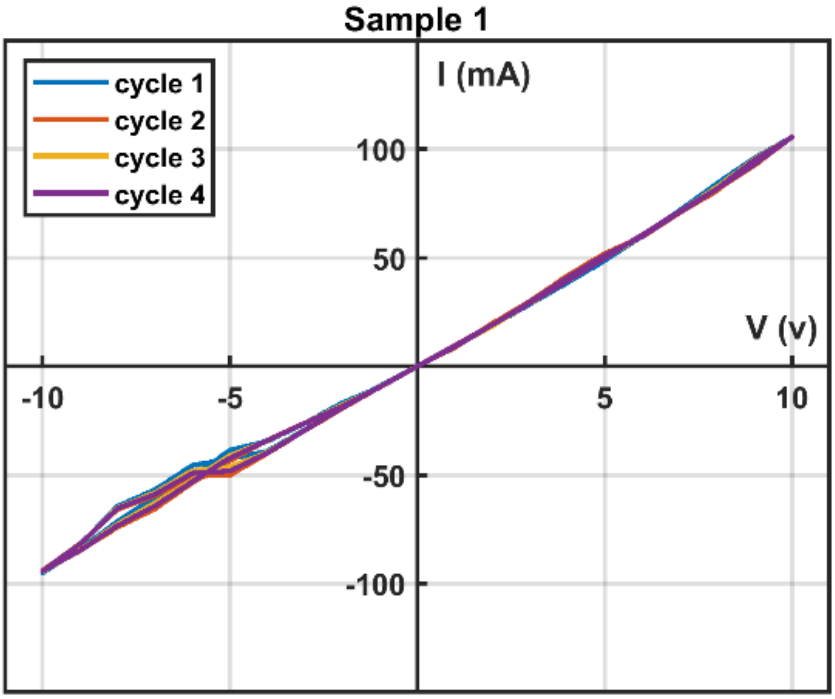


Figure 15. I-V characteristics for sample 1 of ternary system 1, with repeated cycle.

4.2 Ternary system 2

For more cost-effective matter, 3D-Oxides deposited their own bottom electrode of $TiO_2:Nb$ on silicon wafer on which the same ternary thin-film of $Al_2O_3/HfO_2/ZrO_2$ was deposited. This gives an opportunity to understand the variation in the properties with the change in bottom electrode. The samples on the wafers were labelled similar to that of HfO_2 based ternary system 1.

4.2.1 Morphological and composition results

High resolution surface distribution SEM images of bottom electrode should give a clear understanding about the quality of the material, $TiO_2:Nb$ was deposited using CBVD techniques, SEM surface morphology of electrode and its cross-sectional thickness of the sample can be seen in figure 16. Flat granular structures of $TiO_2:Nb$ material is distributed over the visible region with random cracks throughout the surface. A fine tuning of deposition parameters can be adjusted to try and get uniform distribution of the electrode material. The cross-section image of the material shows a significant band with average width of 1 μm.

The deposition of the thin-film material (figure 17), $Al_2O_3/HfO_2/ZrO_2$ is similar to that of ternary system 1 with identical granular patterns can be seen. The distribution is continuous and uniform with average size of these granules to be 100 nm. Thickness of the thin-film is averaged at 205 nm. These measurements show superior surface quality of the thin-film, which is a critical parameter for a manufacturer.

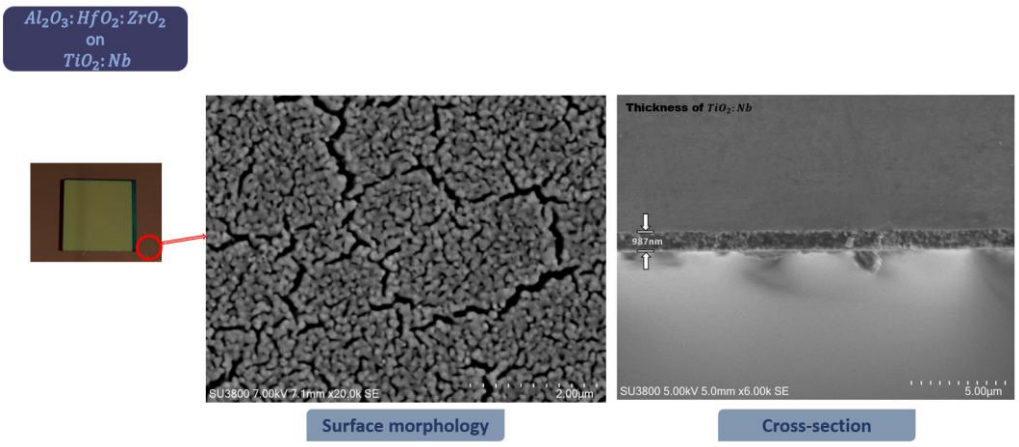


Figure 16. SEM image of surface morphology and cross-section for the electrode material of $TiO_2:Nb$, random distribution of cracks over the distribution of the material with rough pattern can be seen in the surface morphology. Cross-section of the sample with measured marking of the width of electrode is also realized.

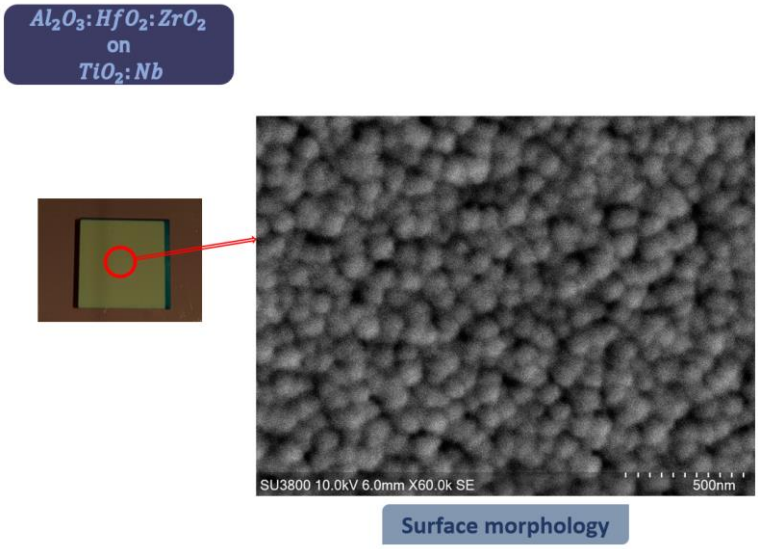


Figure 17. SEM image of the surface morphology of thin-fil material $Al_2O_3/HfO_2/ZrO_2$ on $TiO_2:Nb$.

EDS composition chart in the table 3 gives us an idea of the elements present the thin-film, based on these values one can select the desired samples from the wafer. Site 1 is the ternary thin-film deposition area and site 2 is the bottom electrode area, from the table Here after we can assign S1 which is Zr rich as sample 1, S3 which is 50 – 50 as sample 2, and S4 which is Al rich as sample 3.

Material: $Al_2O_3/HfO_2/ZrO_2$ on $TiO_2:Nb$									
Sample	**composition in At%**								
	site 1						**site 2**		
	O	AL	Zr	Hf	Ti	Nb	O	Ti	Nb
	K line	**Kline**	**L line**	**M line**	**K line**	**L line**	**K line**	**K line**	**L line**
S1	63.24	5.94	13.89	2.97	13.9	NA	65.09	32.77	2.14
S2	64.46	7.81	9.37	2.76	15.61	NA	65.24	32.41	2.35
S3	68.34	7.55	7.2	2.41	14.5	NA	66.95	30.88	2.17
S4	67.23	9.89	4.33	2.28	16.27	NA	65.87	31.51	2.62
S5	65.74	11.43	3.54	2.33	15.09	1.87	67.09	30.29	2.63

Table 3. listing of Al, Zr, and Hf and their composition chart for different samples of the wafer of ternary system 2, site 1 is for the ternary thin-film deposition area and site 2 is for bottom electrode area, K, M, and L-lines are the X-ray lines for inner vacancies (K, M, and L).

4.2.2 Dielectric characterization results

Parameters recorded and analysed are similar to that of ternary system 1. From observing the variations in dielectric constant with frequency from figure 18A, one can observe similar trend of decrease in the values with increase in frequency. They seem to be dropping after 10 kHz. Sample 1 has a maximum dielectric constant of 13 and minimum of 4 (69 % decrease), sample 2 has a higher dielectric constant of 13 and low constant of 3 (76 % decrease), and sample 3 has higher value of 12 and lowest value of 3 (75 % decrease). But only 5 – 10 % variation in dielectric constant between samples at any particular frequencies.

Variation of dissipation loss ($\tan(\delta)$) with frequency in figure 18B, dissipation loss varies different for all three samples but seems to be increasing as frequency increases.

Change in impedance and resistance with frequency in figure 18C and 18D, it is observed that the trend of decrease in the value as frequency increase is the same and we observe the decrease in the value is of the magnitude of 10^2 between maximum and minimum values.

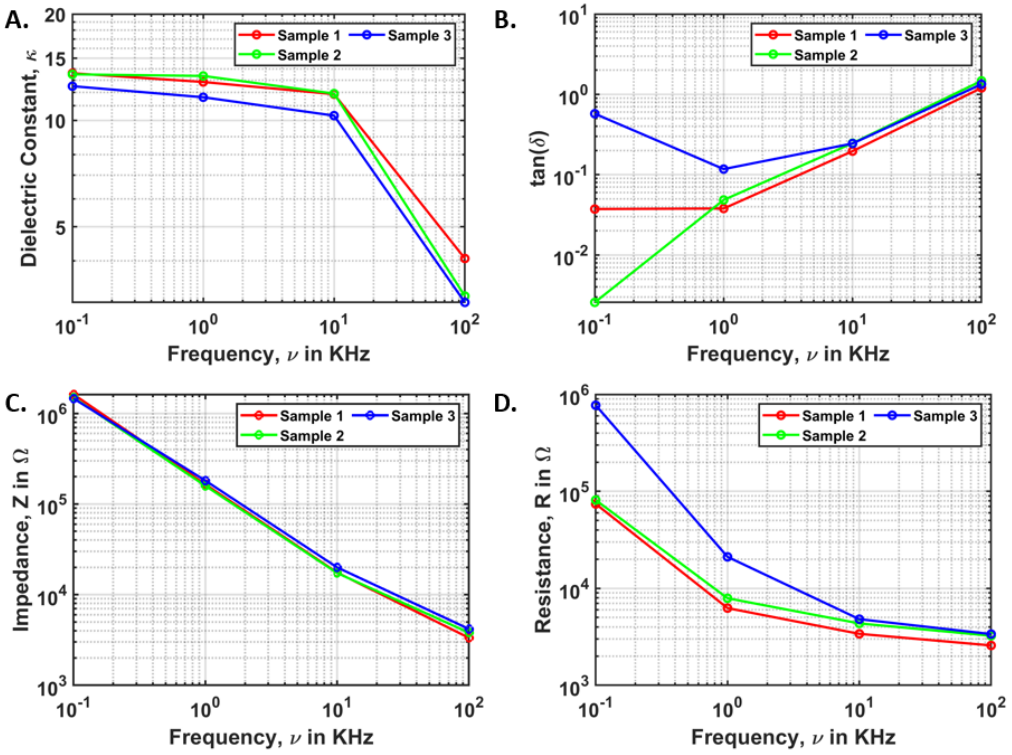


Figure 18. From A to D, we have dielectric constant, dissipation loss $(tan(\delta))$, impedance Z', and resistance and its variation with frequency for sample 1, sample 2, and sample 3.

4.2.3 Influence of external parameters

To study the effect of temperature, three selected samples were placed on the hot plate, before switching it on capacitance and resistance were recorded at room temperature and then these same parameters were recorded for varying temperature of 150, 200, and 250 C.

Variation in capacitance and resistance with frequency and temperature is plotted in figure 19, capacitance seems to be increasing with temperature at lower frequency but at higher frequencies we do observe a revere in trend. But for resistance it was observed that the trend at room temperature is much higher than at any temperature, it can be noted that at higher temperature resistance seems to decrease. The observed changes are consistent with all three samples, but it should be noted for sample 3 the resistance range is decreased by the order of 10^2. These studies of variation in capacitance and resistance with temperature helps us to understand the working mechanism of our device in various temperature ranges.

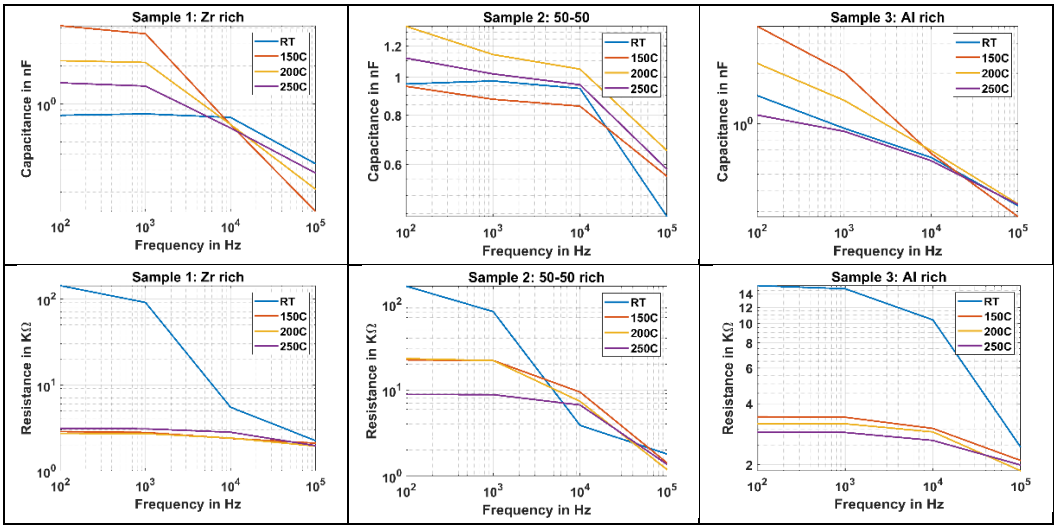


Figure 19. Variation in capacitance and resistance with change in temperature as observed for sample 1, sample 2, and sample 3.

Next, these samples were placed in the glovebox to analyse the variation in controlled environment. Oxygen was completely removed from the box and parameters were recorded. Figure 20 shows this variation in parallel to that of in air for sample 1, sample 2, and sample 3. Capacitance of these samples are relatively high in the air compared to that of in the glovebox.

Dissipation losses seems to be high in air and this decreases as we record it inside a glovebox, but this trend tends to be little-off with sample 2 at lower frequency, we anticipate a mishap in the recording device for this variation. Impedance and resistance in open air has a tendency to decrease with increased frequency, one can still observe this trend even in glovebox expect few exceptional.

From these observations it is clear that the material performs little different under glovebox environment but the trend in variation seems to be similar to most of these cases.

Understanding the external effect of temperature and controlled environment is critical aspect of industrial applications. This gives an opportunity to understand our material properties very well in the uncontrolled environment, PUF greatly depends on randomness in the material and it is essential to understand the variation of these parameters in challenging environment.

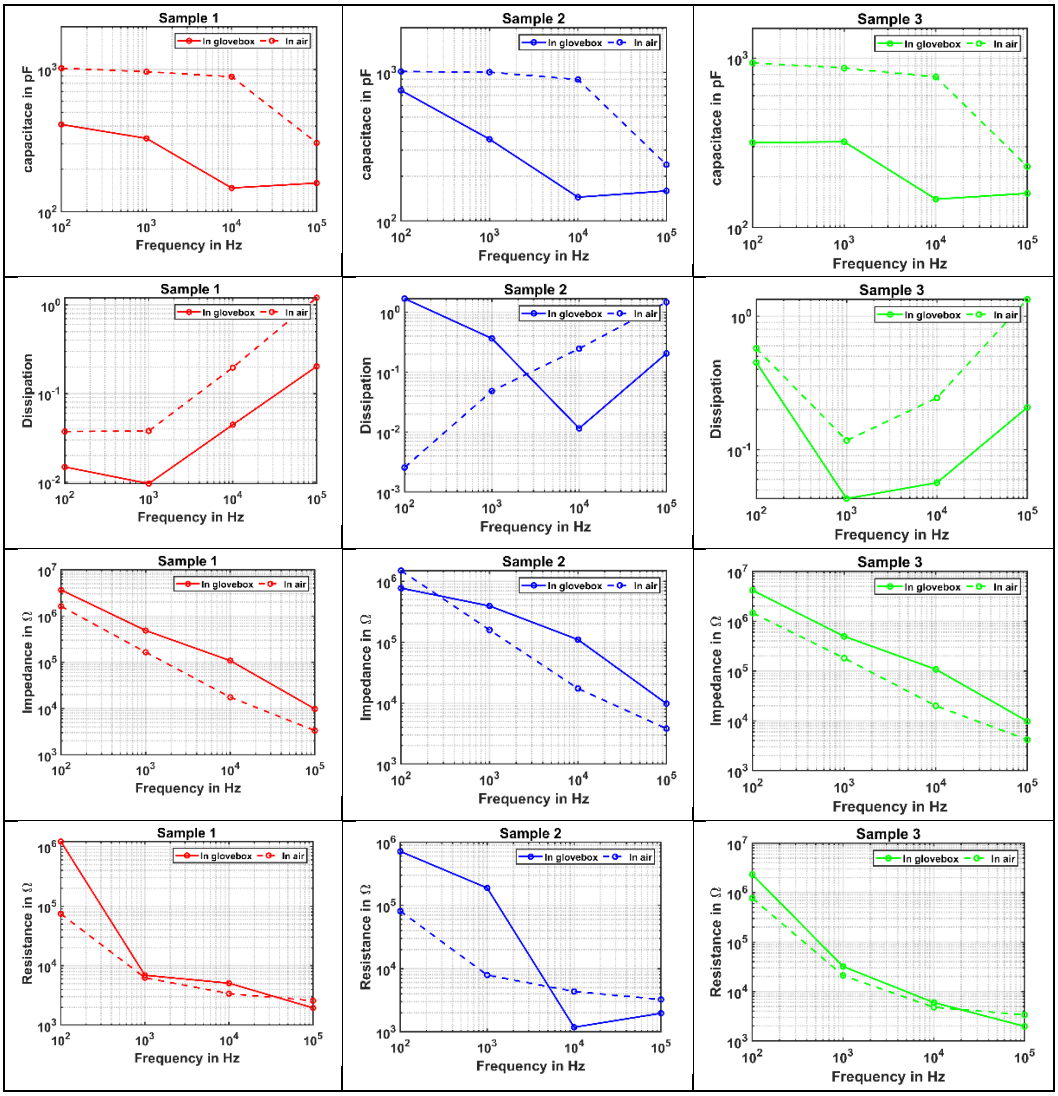


Figure 20. Variation of capacitance, dissipation loss, impedance, and resistance due to frequency for sample 1, sample 2, and sample 3 in glovebox and in open air is plotted for ternary system 2.

4.2.4 I-V characterisation

Figure 21 shows the trend in current for variating DC voltage from $-10\ to\ +10\ V$, for sample 1 at 0 volts we have 0 mA and as voltage increases current increases too, at +10 V we have a maximum current of $1.36\ mA$ but at negative bias it was observed to have -0.46 mA at -10 V.

For sample 2 it was observed that the maximum current of 0.72 mA at +10 volts and at negative bias, it was observed to have $-1.4\ mA$ at -10 volts and for sample 3 we have maximum of $1.4\ mA$ at +10 volts and $-1.08\ mA$ at $-10\ v$.

All three samples have better loop than that of ternary system 1, clear hysteresis behaviour of these samples validate them for the memristive properties of $Hf O_2$. It was observed to have pinched hysteresis loop that is identical to $Hf O_2$ [48] in both positive and negative bias.

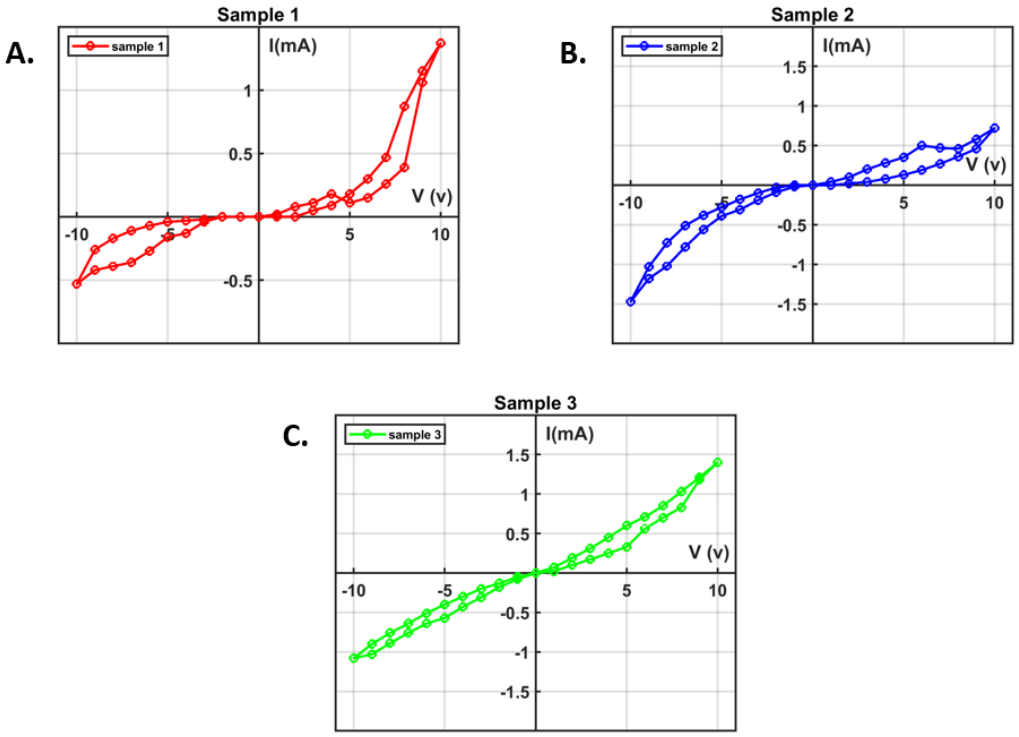


Figure 21. I-V hysteresis plot for a. sample1, b. sample 2, and c. sample 3 of ternary

device 2.

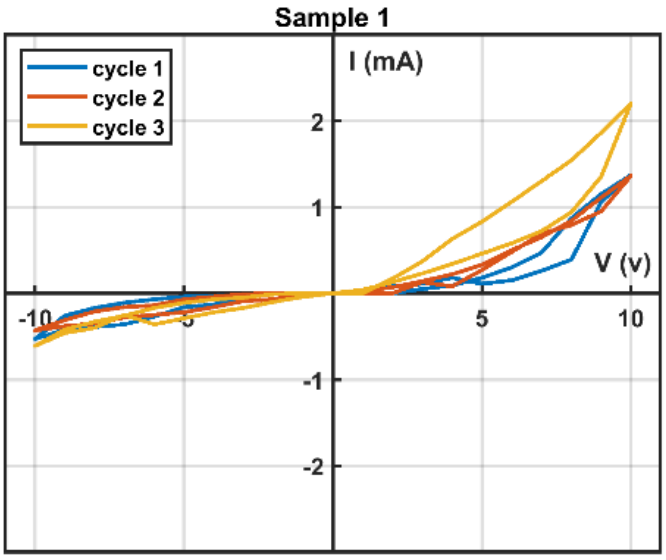


Figure 22. I-V characteristics for sample 1 of ternary system 2, with repeated cycle.

C2C robustness for sample 1 of ternary system 2 was carries out for three cycles and resulting variation in positive bias and negative bias can be clearly observed in figure 22. The changes are much prominent in positive bias with maximum current value is seen between $+5$ and $+10\ V$,

4.3 Implication of observed variation in dielectric properties for PUF application

Critical factor for PUF lies in the degree of the variation in the material from one measured value to another. Not all material properties can be used to derive PUFs, even using certain parameter seems to be good option, one need to consider the complexity in the device. Intrinsic PUFs are much more cost effective rather than designing an extrinsic PUFs. Table 4 provides the variation percent between maximum and minimum values of the parameters measured.

For all these parameters, one can use four frequency ranges available in the LCR device to toggle between minimum and maximum values. The sensitivity in measurement depends upon the detection system that is used. It should also be noted that the minute variation in the thickness and composition can vary these percentages.

Parameters	Samples	variation percentage
Capacitance	sample 1	16.87
	sample 2	25.4
	sample 3	32.198
Dissipation loss	sample 1	125.6
	sample 2	58.58
	sample 3	57.3
Impedance	sample 1	89762.8
	sample 2	81433.1
	sample 3	79003.1
Resistance	sample 1	308768
	sample 2	37391.5
	sample 3	42734

Table 4. variation percentage for parameters between their minimum and maximum value for ternary system 1.

Similar to ternary system 1, percentage variation in ternary system 2 from table 5 we can conclude the same observation. But the advantage of ternary system 2 over 1 comes from the nature of the IV curve, distinctive switching behaviour can be observed with ternary system 2.

Parameters	Samples	variation percentage
Capacitance	sample 1	161.53
	sample 2	339.13
	sample 3	322.727
Dissipation loss	sample 1	3900
	sample 2	73400
	sample 3	1109.09
Impedance	sample 1	48415.2
	sample 2	39229.3
	sample 3	34811.7
Resistance	sample 1	2780.78
	sample 2	2409.27
	sample 3	22820.2

***Table 5*. variation percentage for parameters between their minimum and maximum value for ternary system 2.**

Main focus can be diverted to use distinct IV behaviour of the material 1 and 2 to create memristor PUF, the filamentary-based switching mechanism can be very probabilistic and uncontrolled, which contributes to the final random sequence, depending on the material composition and the fabrication procedure used. IV plots for sample 1 ternary system 2 shows prominent shift in the loop as voltage decrease from +10 to +5 volts.

The variation percentage in the table is the percentage difference between maximum value to the minimum value recorded for particular material properties, i.e., once the acquisition of properties for all four frequencies are acquire, the difference in minimum and maximum value in the acquisition is noted to calculate these percentages. These variations are unique to this particular system, one can expect unique responses in these values for particular frequency challenges.

One can play with frequency to create unique responses in property for these materials. This variation is also subjected to the composition ratio of the material. Based on the type of PUF one can chose the suitable material by studying the variation in material properties from table 5 and 6.

Variation of electrical properties with change in bottom electrode of TiN (ternary system 1) and TiO_2: Nb (ternary system 2) can be seen from table 4 and 5, variation in capacitance is much better in ternary system 2 compared to that of system 1. But variation is resistance, impedance, and losses are better in system 1.

For example, an arbitrary PUF theory can be tested on the sample 1 of ternary system 2, due to its large variation percentage of resistance in the system. IV characterisation can be carried on to confirm this variation, C2C analysis of the sample furthers proves the randomness in the measurement that is unique to the material.

One can also use the variation in capacitance properties for coating PUF application. Thin-film coating of ternary system with varied composition ratio ensures the value difference in measurements from one spot to another spot. Further variation in thickness can add additional complexity that is unique to the PUF.

Further variation can be achieved with experimenting with temperature and environment. Variation of material properties with temperature and controlled environment is always anticipated, studying this variation for the thin-film can make us understand the possible application domain and properties to use under certain conditions. PUFs can be designed keeping this variation in mind to work in extreme condition without the fear of failure.

5. Optical PUF

Non-sequential modelling of the optical system helps us to understand the scattering and illumination by the system. Our physical system consists of LED diode, thin-film, and CMOS sensor as a PUF setup, each of these stacks need to be thoroughly understood to model the system. Physical PUF setup being used is an optical system with three main layers and it is essential to understand them well in-order to model the system. The OLED screen consists of red, green and blue LEDs of size 50 μm x 190 μm that are distributed with constant pitch of 20 μm along X and Y direction. Each LEDs can be handled according to the user's desires using Raspberry module. This is followed by uniform deposition of thin-film material of thickness 450 nm on 0.8 mm glass slab which are separated by a distance of 2.7 mm from OLED display. Raspberry Pi camera (CMOS) of 3280 (H) x 2464 (V) active pixels of size 1.12 μm is place just below the slab is then used as the detector (refer figure 23).

Light is emitted from LEDs of OLED display which then passes through TiO_2 thin-film which indeed create characteristic changes in transmitted light that are observed using CMOS. To quantify and speculate these characteristics one can use Zemax to model the system.

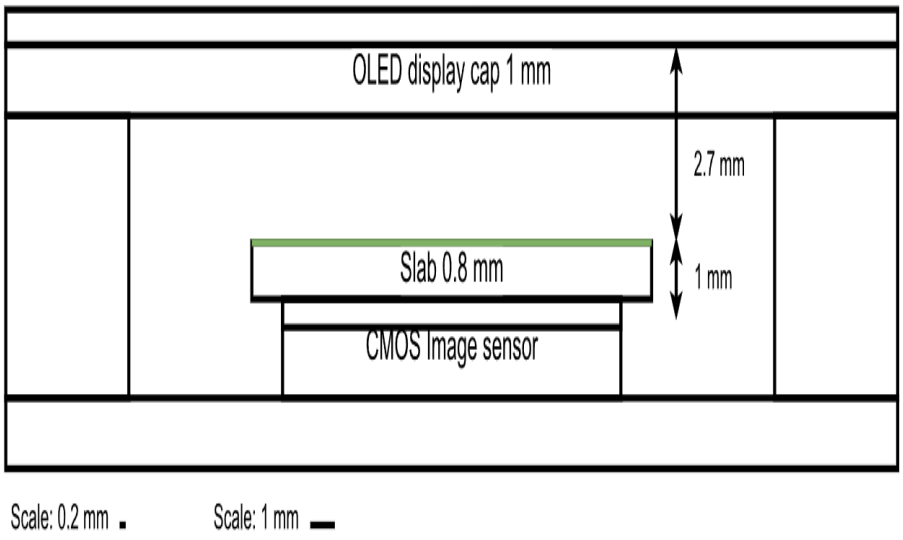


Figure 23. Schematic of three main layers of Optical system having OLED, glass slab and CMOS image sensor with specific distance of separation.

To model the LED light sources it is first essential to calculate beam divergence, this is not an easy task as it involves the individual manipulation of LEDs inside the OLED display. Python code to handle these LEDs were scripted and raw data from the CMOS was acquired for individual red, blue, and green LEDs in the center. This was done in order to eliminate the edge effect in the CMOS sensors.

5.1 Divergence study:

Raspberry Pi camera module was directly strapped on top of OLED display and distance between them was measured to be 0.9 mm. an acquisition was made using Raspberry Pi micro-computer module to find row and column on OLED for which complete light spot can be observed on CMOS. Several combinations of acquisition were made using different colors of LED at different suitable spots to check the reliability and similarity between similar LEDs. Once data from acquisition are acquired, they were processed in MATLAB to visualize (figure 24.) and then analyze.

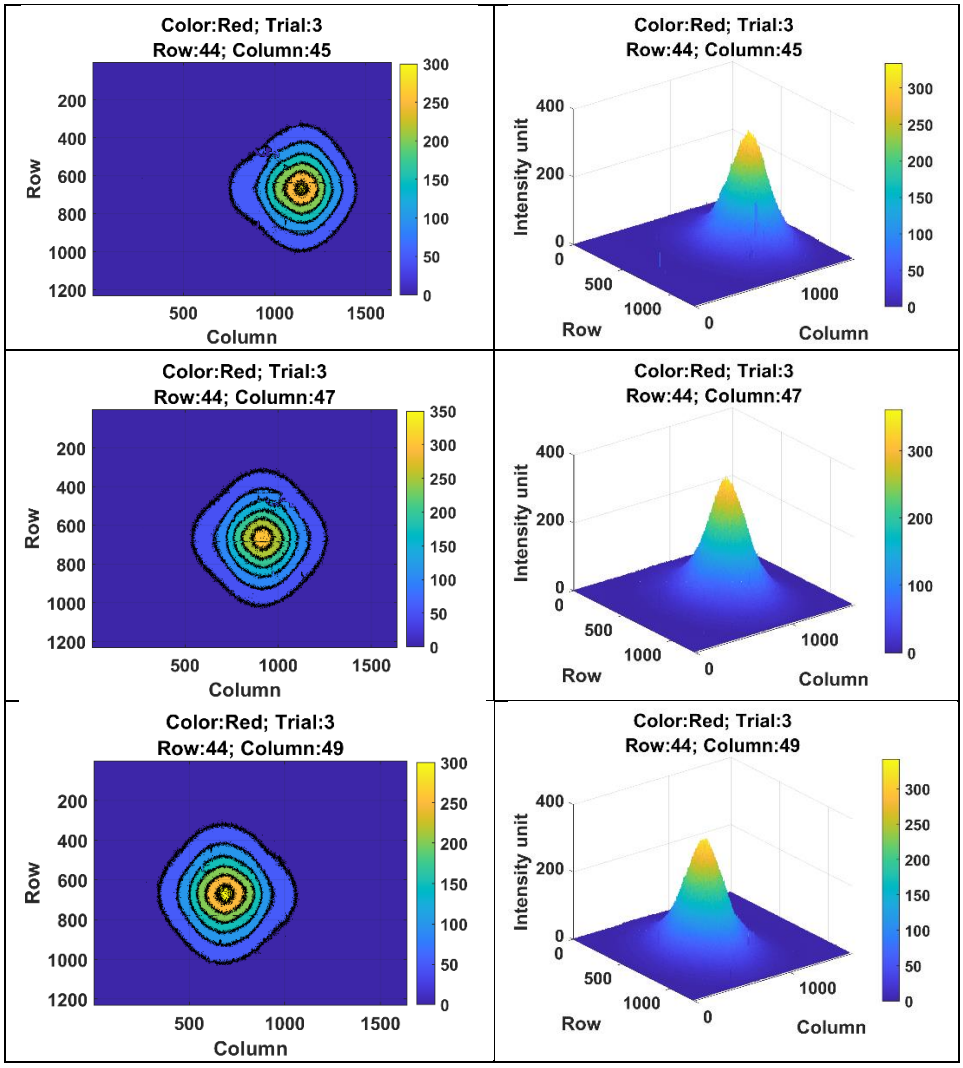


Figure 24. 2D and 3D contour distribution of red LED illumination at three different positions of columns 45, 47, 49 and row 44.

The acquisition was conducted for shutter speed of 47900 micro second of red, blue and green LEDs at different positions of OLED display. The data obtained from acquisition are of 2464 x 3280 array which consists data from of Bayer pattern of blue, green and red photocells distributed in different orders. Once this point was noticed, the new array for only active photocell of specific colors for same color

illumination were created. i.e., for red LED illumination only array of red photocells was considered. To extract divergence, one need to calculate beam diameter in standard units, for this it is necessary to multiply beam diameter by a value of 2.24 µm, correction factor due to the omission of irrelevant detector pixels in the area. From figure 24. we can see the distribution shift for red LED at three different positions (represented as (row, column)) of (44,45), (44,47), and (44,49). One can observe in all pictures the distribution along X and Y are not same and it varies accordingly to the position of LED. In addition to this one can also observe dust particles, flickering in the distribution. An attempt was made to measure beam divergence along X and Y by fitting the Gaussian distribution and then calculating beam diameter to finally calculate beam divergence (figure 25).

Slight ellipticity in the red LEDs beam can be observed in figure 25, for which variation in divergence is around 2 – 3 degrees. Distribution along X is wider compared to that of Y direction. Apart from ellipticity it is observed to have slight change in shape along X at positions (44, 45) and (44, 49). In table 6 it is listed the divergence along X and Y, and maximum intensity value for three different colors of LEDs. Several trials were carried and two of them are tabulated.

colour	Trial	position		Divergence in degree		Max intensity value
		Row	Column	Along X	Along Y	
Red	1	44	45	84	82	350
		44	47	84	82	
		44	49	86	83	
	2	44	45	84	82	
		44	47	84	82	
		44	49	86	83	
Green	1	44	45	78	74	550
		44	47	79	75	
		44	49	79	76	
	2	44	45	77	74	
		44	47	77	74	
		44	49	79	76	
Blue	1	44	45	82	73	450
		44	47	74	75	
		44	49	82	74	
	2	44	45	82	73	
		44	47	74	74	
		44	49	82	74	

Table 6. List of divergence and intensity values for three different positions of three different color LEDs

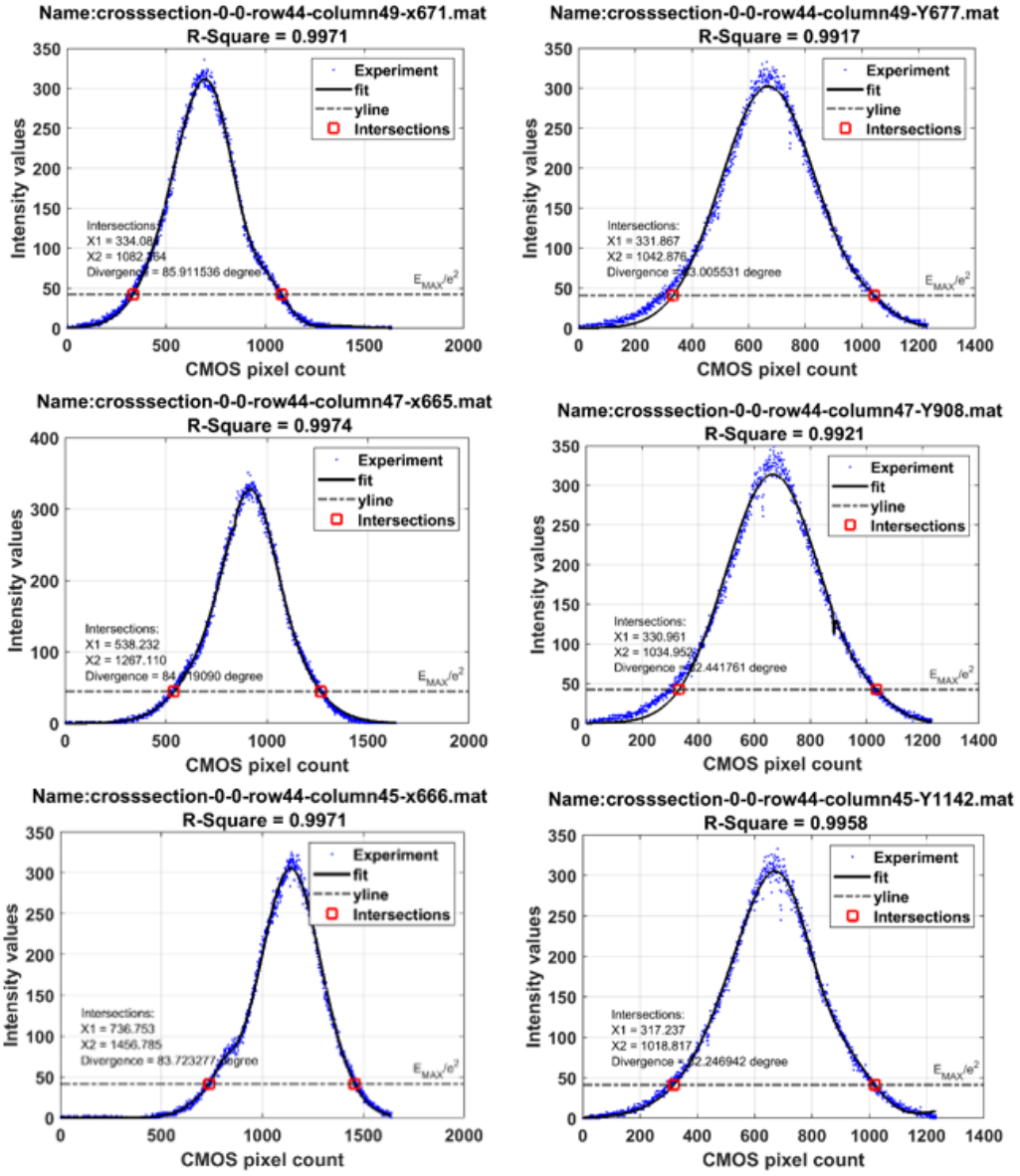


Figure 25. Fitted distribution plots of intensity values along X and Y of CMOS plane for illumination of red LED at three different positions of (44,45), (44,47), (44,49) on OLED display with their corresponding divergence value, x and y followed by the number in the name of the plot refer to the X and Y position in CMOS along which the acquisition was made.

5.2 Zemax simulation for irradiance analysis for a modelled miniaturized system

From the above observations an attempt was made to find the best parameters at which a distinct interference patterns can be observed. The system was modelled to miniaturize the existing physical system of integrated optical PUF for which non-sequential simulations were carried on.

For miniaturizing the model, the simulation was designed to have a dimension of 1 mm x 1mm between which different stacks of LEDs, material and CMOS are place. They are equally separated by the distance of 0.5 mm.

Square LEDs are modeled to have a dimension of 10 x 10 um, which emits wavelength at 550 nm and have divergence of 80 degrees [ref table 6] along X and Y, power for these LEDs is fixed at 1 milliwatts. Position of these LEDs [ref Table 7] are changed to see the effect of transmission through patterned thin-film on interference intensities.

Patterned thin-film of 1 x 1 mm was designed with checkered pattern that have individual dimension of 0.25 x 0.25 mm of BK7 glass of thickness 0.1 mm. These patterned cells have a variation in refractive index, dark colored cells are of 1.99 and white cells are of 1, ref. figure 26. These are the coatings that are placed on top of 0.1mm glass substrate.

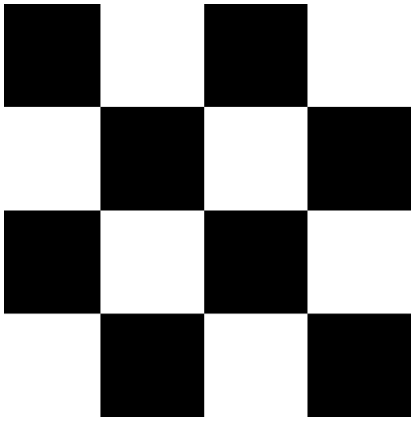


Figure 26. Schematic of modeled checkered patterned thin-film coating of 4x4 cells of dimension 0.25 mm where refractive index of black cell is 1.99 and white cell with 1.

Two coherent light sources separated by certain distance on a plane to produce interference pattern and this plays an important role in generating responses. The subtle difference in interference can determined what kind of PUF it can be used as. Square detector of dimension 1 x 1 mm was created with 1000 x 1000 pixels along x and y direction.

Position	LED	X in mm	Y in mm
1	1	0.01	0
	2	-0.01	0
2	1	0.01	0.01
	2	-0.01	-0.01
3	1	0.01	0.5
	2	-0.01	0.5

Table 7. Placed position of LEDs as entered in the Zemax OpticStudio software to place them at three different configuration positions.

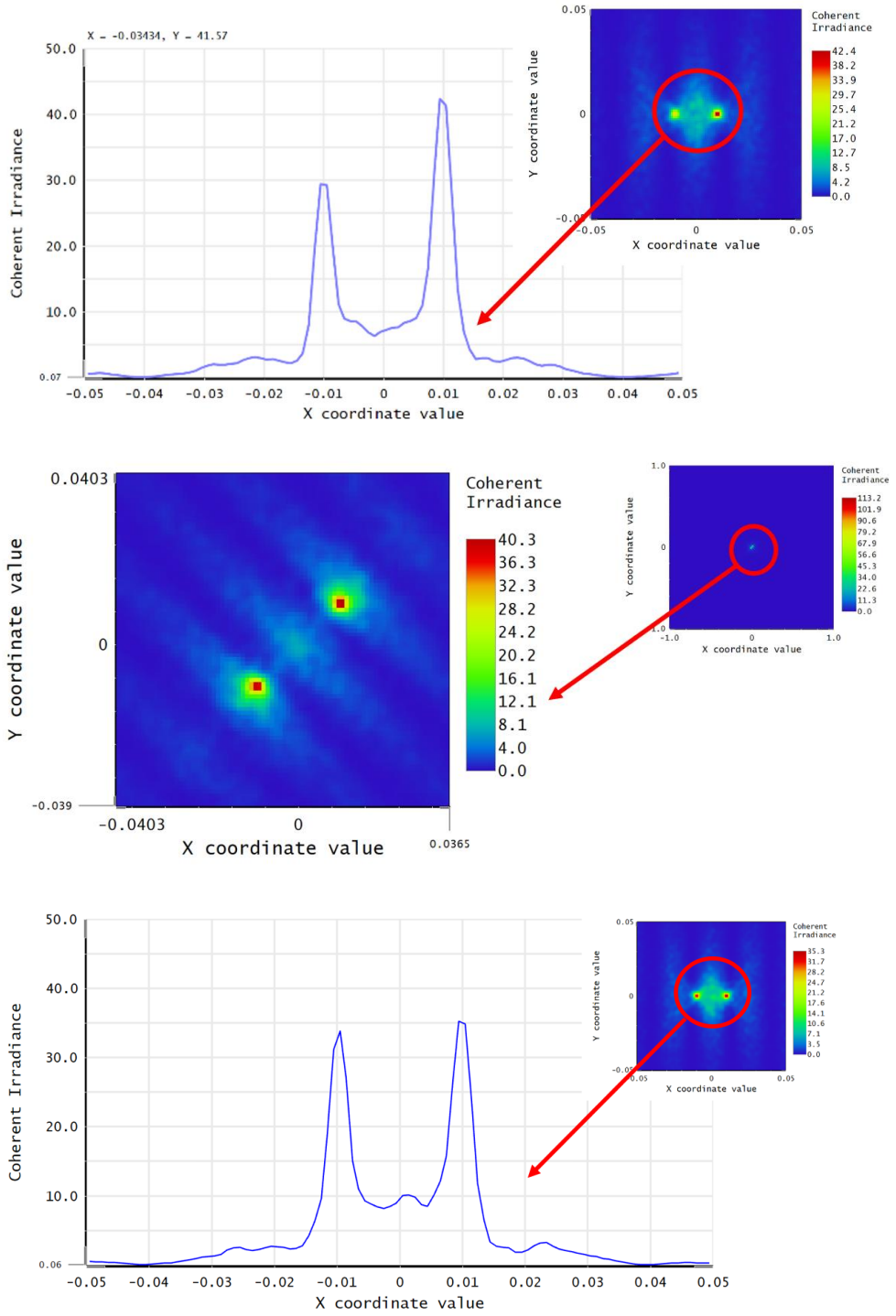


Figure 27. From top to bottom, coherent irradiance plot at position 1 for the cross-section along x (row), false color coherent irradiance map showing diagonal distribution of interference pattern at position 2, coherent irradiance plot at position 3 for the cross-section along x.

Coherent irradiation plot seen in figure 27 shows subtle variation in the interference pattern for the variation in LEDs position, this is expected as the checkered slab acts as our patterned thin-film and variation refractive index gives uniqueness to the transmission. This can be observed with cross-sectional irradiation plots from position 1 to position 3. This is unique to this setup and with certain variation in patterned thin-film one can expect unique transmittance pattern for that material.

These simulations provide some preliminary idea of what the propagation might look like for a miniaturized system, the illumination pattern simulated can be used to calculate the variation. This initial finding for few sets of parameters has proven to be most efficient way of dealing with optical system to clearly understand what to expect before going to manufacturing process. But it should be noted that Zemax lacks the ability to deal with modeling of such a complex thin-film, still a relatively close coating can be created to understand how the propagation of the light will be with certain variation to the actual system.

6. Limitation of the study and future perspective

Ternary HfO_2 device 1 and 2, i.e., $Al_2O_3/HfO_2/ZrO_2$ on TiN and $Al_2O_3/HfO_2/ZrO_2$ on $TiO_2{:}Nb$ are studied in the same way. EDS composition analysis of ternary system 1 and 2 showed ~1.3 and ~2.5 At% of hafnium respectively, this directly relates to the fact that the dielectric constant for these materials were capped at 15. Future batch of production can ensure the increase in percentage to observe prominent values for other electrical application like MIM capacitor.

Using silver for the top electrode sometimes adversely affect the dielectric properties of the devices, and manually putting the electrodes will make it difficult to have one-one comparison. Even the slightest variation in the area of the electrode has proven to affect the capacitance of the system drastically. This can be overcome by standardizing a method to deposit a top electrode, such as spluttering.

Due to lack of IV analyser, it is hard to conduct more cycles of acquisitions with added precision. The recorded IV characteristic plots can lead to a possible application to the PUF but further study need to be done by using NIST 800-22 [56], a 15-test series package that can be used to evaluate the randomness of bit sequences produced by either hardware or software cryptographic systems.

The randomness in material properties for electrical PUFs are subjected to machine-learning attacks. One need to create more CRPs to overcome this issue, this can be done using optical PUFs.

More modelling using Zemax need to be carried out by varying and fine tuning the parameters. Better modelling of the material needs to be carried first, upon which ray tracing can be carried on to know the behaviour and trend of the light propagation in the thin-film.

Other than these critical points one need to note the environmental, manual, experimental and manufacturing errors influencing the experiment for some extent, cautious approaches were implemented then and there as the error took place.

7. Conclusion

The thesis itself carries in a way to convey the importance of material characterisation for PUF application, affordable HfO_2 based ternary system 1, $Al_2O_3/HfO_2/ZrO_2$ on TiN and ternary system 2, $Al_2O_3/HfO_2/ZrO_2$ on $TiO_2{:}Nb$ provide an idea of change that one can expect with certain variation in material parameters. Effect of composition on thin-films electrical properties like capacitance, dissipation loss, impedance, and resistance were studied and tabulated.

SEM imaging of surface morphology of ternary 1 and ternary 2 devices show the superior manufacturing qualities using CBVD techniques to obtain very uniform thin-films. Further analysis of in-house electrodes like $TiO_2{:}Nb$ shows promising results for future improvements of this material. Close study of the composition percentages of thin-film using EDS analysis helps us to select only necessary samples to characterize, hence minimizing both time and resources it would have cost to analyse them all. This on other hand is also helpful in noting down the best composition sample and them optimizing the deposition to get more of this sample. SEM images provide assurance to ensure quality of 3D-Oxide.

Dielectric characterisation of ternary system 1 and 2 give us an idea of what material parameters like capacitance, resistance, impedance, or dissipation losses can offer to fabricate devices for specific application. Large variation in the impedance and resistance value at lower frequency, and trend of decrease in these properties for increase in frequency.

Effect of bottom electrode i.e., TiN and $TiO_2{:}Nb$ on dielectric properties were thoroughly studied and ternary system of Al2O3/HfO_2/ZrO2 on $TiO_2{:}Nb$ has proven to have better capacitance to that of a system on TiN, this is encouraging for the company as it is deposited in-house which means it is much more time effective and cost-effective. Variation in capacitance in ternary system 2 is much superior to that of ternary system 2 and this can be used in coating PUF application.

Variation of material properties under challenging conditions, such as varied temperature and glovebox environment is studies, this can be used to design PUFs under challenging environments.

IV characterisation of ternary system 1 and 2 leads to an important discovery of hysteresis loop and C2C variation that is unique to the material which can be used to derive memristor-PUFs.

Numerical simulations were carried out to the existing optical PUF system, first by analysing the divergence of red, blue, and green LEDs of the OLED display and then using this data preliminary modelling of miniature system was realized. Further, ray tracing was performed for this to analyse the irradiance plot of the system. This helps to understand what parameters one can use to realize and extract unique transmittance intensities for PUFs application.

Overall, this thesis helps to understand the variation of properties within a thin-film material and variation compared to an another thin-film material that can be used for certain PUF application.

References

1. R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 1st ed. Wiley, 2020. doi: 10.1002/9781119644682.
2. G. Khalil, R. Doss, and M. Chowdhury, "A Comparison Survey Study on RFID Based Anti-Counterfeiting Systems," JSAN, vol. 8, no. 3, p. 37, Jul. 2019, doi: 10.3390/jsan8030037.
3. P. Randhawa, R. J. Calantone, and C. M. Voorhees, "The pursuit of counterfeited luxury: An examination of the negative side effects of close consumer–brand connections," Journal of Business Research, vol. 68, no. 11, pp. 2395–2403, Nov. 2015, doi: 10.1016/j.jbusres.2015.02.022.
4. "The Economic Impacts of Counterfeiting and Piracy," ICC - International Chamber of Commerce. https://iccwbo.org/publication/economic-impacts-counterfeiting-piracy-report-prepared-bascap-inta (accessed Aug. 09, 2022).
5. "Counterfeit medical products", World health organization. https://apps.who.int/gb/archive/pdf_files/A61/A61_16-en.pdf
6. J. Zindy, *Livre blanc - Cybers´ecurit´e des syst`emes industriels et techniques*. EIFFAGE ENERGIE SYSTEMES -CLEMESSY. Contact: jocelyn.zindy@eiffage.com
7. "Cybersecurity Barometer 2018 | Orange Business Services." http://www.orange-business.com/fr/mediatheque/brochure/barometre-cybersecurite-2018 (accessed Aug. 09, 2022).
8. R. Arppe and T. J. Sørensen, "Physical unclonable functions generated through chemical methods for anti-counterfeiting," *Nat Rev Chem*, vol. 1, no. 4, Art. no. 4, Apr. 2017, doi: 10.1038/s41570-017-0031.
9. "How to implement security by design for IoT," *ENISA*. https://www.enisa.europa.eu/news/enisa-news/how-to-implement-security-by-design-for-iot (accessed Aug. 09, 2022).
10. E. E. C. S. P. (EECSP), Cyber Security in the Energy Sector," tech. rep., Energy Expert Cyber Security Platform (EECSP), Feb. 2017.
11. P. A. overview of the I. S. M. R. 2017-2022 – indiz.de, "An overview of the IoT Security Market Report 2017-2022," *IIoT World*, Nov. 25, 2017. https://www.iiot-world.com/news/reports/an-overview-of-the-iot-security-market-report-2017-2022/ (accessed Aug. 09, 2022).
12. "Physical Unclonable Functions and Applications: A Tutorial | IEEE Journals & Magazine | IEEE Xplore." https://ieeexplore.ieee.org/document/6823677 (accessed Aug. 09, 2022).

13. R. Maes and I. Verbauwhede, “Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions,” in *Towards Hardware-Intrinsic Security: Foundations and Practice*, A.-R. Sadeghi and D. Naccache, Eds. Berlin, Heidelberg: Springer, 2010, pp. 3–37. doi: 10.1007/978-3-642-14452-3_1.

14. X. Xu, W. Burleson, and D. E. Holcomb, “Using Statistical Models to Improve the Reliability of Delay-Based PUFs,” in *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, Jul. 2016, pp. 547–552. doi: 10.1109/ISVLSI.2016.125.

15. N. N. Anandakumar, M. S. Hashmi, and S. K. Sanadhya, “Compact Implementations of FPGA-based PUFs with Enhanced Performance,” in *2017 30th International Conference on VLSI Design and 2017 16th International Conference on Embedded Systems (VLSID)*, Jan. 2017, pp. 161–166. doi: 10.1109/VLSID.2017.7.

16. A. Priadarshini and M. Jagadeeswari, “Low power reconfigurable FPGA based on SRAM,” in *2013 International Conference on Computer Communication and Informatics*, Coimbatore, Tamil Nadu, India, Jan. 2013, pp. 1–6. doi: 10.1109/ICCCI.2013.6466160.

17. R. Maes, A. Van Herrewege, and I. Verbauwhede, “PUFKY: A Fully Functional PUF-Based Cryptographic Key Generator,” in *Cryptographic Hardware and Embedded Systems – CHES 2012*, Berlin, Heidelberg, 2012, pp. 302–319. doi: 10.1007/978-3-642-33027-8_18.

18. G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in *Proceedings of the 44th annual Design Automation Conference*, New York, NY, USA, Jun. 2007, pp. 9–14. doi: 10.1145/1278480.1278484.

19. N. Beckmann and M. Potkonjak, “Hardware-Based Public-Key Cryptography with Public Physically Unclonable Functions,” in *Information Hiding*, Berlin, Heidelberg, 2009, pp. 206–220. doi: 10.1007/978-3-642-04431-1_15.

20. L. Bolotnyy and G. Robins, “Physically Unclonable Function-Based Security and Privacy in RFID Systems,” in *Fifth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom’07)*, Mar. 2007, pp. 211–220. doi: 10.1109/PERCOM.2007.26.

21. J. Guajardo, S. S. Kumar, G. Schrijen, and P. Tuyls, “Physical Unclonable Functions and Public-Key Crypto for FPGA IP Protection,” *2007 International Conference on Field Programmable Logic and Applications*, 2007, doi: 10.1109/FPL.2007.4380646.

22. K. Kursawe, A.-R. Sadeghi, D. Schellekens, B. Skoric, and P. Tuyls, “Reconfigurable Physical Unclonable Functions - Enabling technology for tamper-resistant

storage," in *2009 IEEE International Workshop on Hardware-Oriented Security and Trust*, Jul. 2009, pp. 22–29. doi: 10.1109/HST.2009.5225058.

23. U. Rührmair and D. E. Holcomb, "PUFs at a glance," in *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Mar. 2014, pp. 1–6. doi: 10.7873/DATE.2014.360.

24. Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Emerging Physical Unclonable Functions With Nanotechnology," *IEEE Access*, vol. 4, pp. 61–80, 2016, doi: 10.1109/ACCESS.2015.2503432.

25. Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Memristive crypto primitive for building highly secure physical unclonable functions," *Sci Rep*, vol. 5, no. 1, Art. no. 1, Aug. 2015, doi: 10.1038/srep12785.

26. H. M. Ibrahim, H. Abunahla, B. Mohammad, and H. AlKhzaimi, "Memristor-based PUF for lightweight cryptographic randomness," *Sci Rep*, vol. 12, no. 1, Art. no. 1, May 2022, doi: 10.1038/s41598-022-11240-6.

27. E. Wagner *et al.*, "Geometry of Chemical Beam Vapor Deposition System for Efficient Combinatorial Investigations of Thin Oxide Films: Deposited Film Properties versus Precursor Flow Simulations," *ACS Comb Sci*, vol. 18, no. 3, pp. 154–161, Mar. 2016, doi: 10.1021/acscombsci.5b00146.

28. D. Bijou *et al.*, "Study of titanium amino-alkoxide derivatives as TiO2 Chemical Beam Vapour Deposition precursor," *Materials Chemistry and Physics*, vol. 277, p. 125561, Feb. 2022, doi: 10.1016/j.matchemphys.2021.125561.

29. G. Benvenuti, E. Halary-Wagner, A. Brioude, and P. Hoffmann, "High uniformity deposition with chemical beams in high vacuum," *Thin Solid Films*, vol. 427, no. 1, pp. 411–416, Mar. 2003, doi: 10.1016/S0040-6090(02)01190-2.

30. J. E. Mahan, Physical Vapor Deposition of Thin Films. 2000. Accessed: Aug. 16, 2022. [Online]. Available: https://ui.adsabs.harvard.edu/abs/2000pvdt.book.....M

31. J.-H. Park and T. S. Sudarshan, *Chemical Vapor Deposition*. ASM International, 2001.

32. "Atomic Layer Deposition: An Overview | Chemical Reviews." https://pubs.acs.org/doi/full/10.1021/cr900056b?casa_token=UuPJwHMNGssAAAAA:9_dkNYpxc-PQ8ecs6wbfDhIdHGqvquye82XCqEFjCrhVO9iPktXylxDP39TJRwJT13mfJw7yEuY-6pQ (accessed Aug. 16, 2022).

33. K. L. Choy, "Chemical vapour deposition of coatings," Progress in Materials Science, vol. 48, no. 2, pp. 57–170, Jan. 2003, doi: https://doi.org/10.1016/S0079-6425(01)00009-3

34. "Molecular Beam Epitaxy - 1st Edition." https://www.elsevier.com/books/molecular-beam-epitaxy/henini/978-0-12-387839-7 (accessed Aug. 16, 2022).

35. P. W. Atkins, J. De Paula, and J. Keeler, Atkins' physical chemistry. Oxford: Oxford University Press, 2019.

36. I. Novak, "From the Arrhenius to the Clausius–Clapeyron Equation," Chem. Educator, vol. 7, no. 6, pp. 347–348, Dec. 2002, doi: https://doi.org/10.1007/s00897020617a.

37. Laidler, "Chemical Kinetics 4th Edition." https://pdf.wecabrio.com/laidler-chemical-kinetics-4th-edition.pdf (accessed Aug. 16, 2022).

38. A. Dabirian, Y. Kuzminykh, E. Wagner, G. Benvenuti, S. A. Rushworth, and P. Hoffmann, "Chemical Vapor Deposition Kinetics and Localized Growth Regimes in Combinatorial Experiments," ChemPhysChem, vol. 12, no. 18, pp. 3524–3528, 2011, doi: 10.1002/cphc.201100637.

39. M. Reinke, Y. Kuzminykh, and P. Hoffmann, "Surface Reaction Kinetics of Titanium Isopropoxide and Water in Atomic Layer Deposition," J. Phys. Chem. C, vol. 120, no. 8, pp. 4337–4344, Mar. 2016, doi: 10.1021/acs.jpcc.5b10529.

40. E. Wagner, C. S. Sandu, S. Harada, G. Benvenuti, V. Savu, and P. Muralt, "Fabrication of complex oxide microstructures by combinatorial chemical beam vapour deposition through stencil masks," Thin Solid Films, vol. 586, pp. 64–69, Jul. 2015, doi: 10.1016/j.tsf.2015.04.021.

41. T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A PUF taxonomy," Applied Physics Reviews, vol. 6, no. 1, p. 011303, Mar. 2019, doi: 10.1063/1.5079407.

42. L. Bossuet, X. T. Ngo, Z. Cherif, and V. Fischer, "A PUF Based on a Transient Effect Ring Oscillator and Insensitive to Locking Phenomenon," IEEE Transactions on Emerging Topics in Computing, vol. 2, no. 1, pp. 30–36, Mar. 2014, doi: 10.1109/TETC.2013.2287182.

43. T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama, "A New Arbiter PUF for Enhancing Unpredictability on FPGA," The Scientific World Journal, vol. 2015, p. e864812, Sep. 2015, doi: 10.1155/2015/864812.

44. P. Koeberl, Ü. Kocabaş, and A.-R. Sadeghi, "Memristor PUFs: A new generation of memory-based Physically Unclonable Functions," in 2013 Design, Automation & Test in Europe Conference & Exhibition (DATE), Mar. 2013, pp. 428–431. doi: 10.7873/DATE.2013.096.

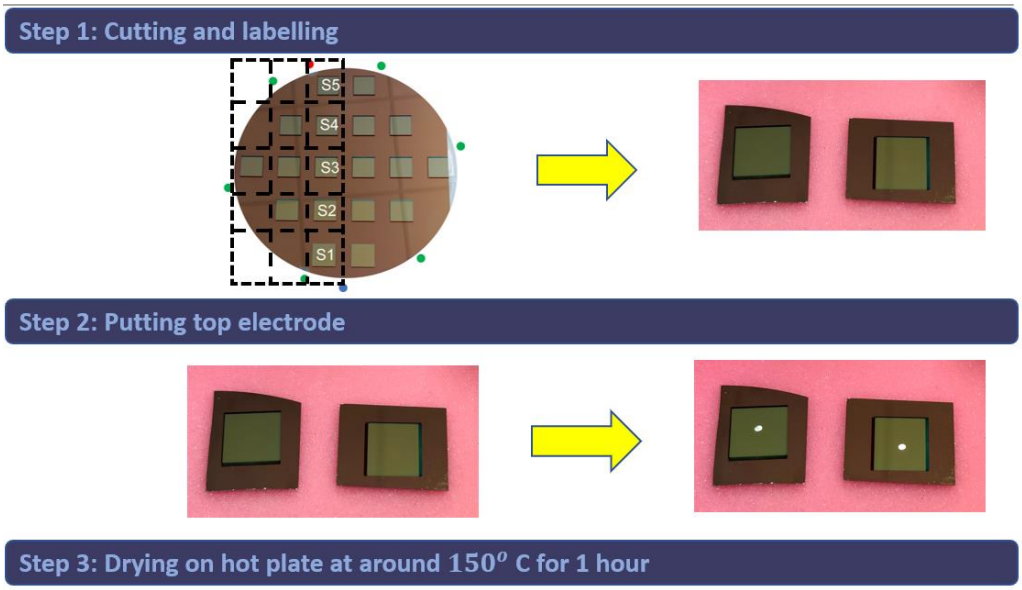
45. P. Tuyls, G.-J. Schrijen, B. Škorić, J. van Geloven, N. Verhaegh, and R. Wolters, "Read-Proof Hardware from Protective Coatings," in Cryptographic Hardware and

Embedded Systems - CHES 2006, Berlin, Heidelberg, 2006, pp. 369–383. doi: 10.1007/11894063_29.

46. J. Roberts et al., "Using Quantum Confinement to Uniquely Identify Devices," Sci Rep, vol. 5, no. 1, Art. no. 1, Nov. 2015, doi: 10.1038/srep16456.
47. M. Housa, High k gate dielectric, IPO, Bristal (2004) Chapter 1
48. Renato Gaudioso," Investigation of electrical properties of HfO_2 thin-film deposited by CBVD", Internship report, 2021, link to this report .
49. J. C. Slater , J. Chem. Phys. 1964, 41, 3199
50. J. Müller et al., "Ferroelectricity in Simple Binary ZrO2 and HfO_2," Nano Lett, vol. 12, no. 8, pp. 4318–4323, Aug. 2012, doi: 10.1021/nl302049k.
51. P. Polakowski et al., "Ferroelectric deep trench capacitors based on $Al:HfO_2$ for 3D nonvolatile memory applications," in 2014 IEEE 6th International Memory Workshop (IMW), May 2014, pp. 1–4. doi: 10.1109/IMW.2014.6849367.
52. S. Balatti, S. Ambrogio, Z. Wang, and D. Ielmini, "True Random Number Generation by Variability of Resistive Switching in Oxide-Based Devices," IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 5, no. 2, pp. 214–221, Jun. 2015, doi: 10.1109/JETCAS.2015.2426492.
53. Z. Wei et al., "True random number generator using current difference based on a fractional stochastic model in 40-nm embedded ReRAM," in 2016 IEEE International Electron Devices Meeting (IEDM), Dec. 2016, p. 4.8.1-4.8.4. doi: 10.1109/IEDM.2016.7838349.
54. H. Jiang et al., "A novel true random number generator based on a stochastic diffusive memristor," Nat Commun, vol. 8, no. 1, Art. no. 1, Oct. 2017, doi: 10.1038/s41467-017-00869-x.
55. Edmund optics, Geometrical Optics 101: Paraxial Ray Tracing Calculations, https://www.edmundoptics.eu/knowledge-center/application-notes/optics/geometricaloptics-101-paraxial-ray-tracing-calculations/
56. Rukhin, A. et al. Nist special publication 800-22: A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications. In NIST Special Publication 800-22 (2010).

Appendices

Appendix A. Preparing the samples for dielectric characterisation



Probing setup to insert these thin films to connect to an LCR meter is as shown in figure 1.

Figure 1. self-made probing setup using wooden base and paper metal clips.

Appendix B. BK Precision's 880 LCR meter

Figure 1. Photo-clip of portable BK precisions 880 LCR meter

Handheld highly portable (figure 1) LCR meter 880 from BK precision is designed to measure primary parameters like inductance, capacitance, resistance, impedance, and Direct Current Resistance (DCR) and secondary parameters like dissipation, quality factor, phase angle and Equivalent Series Resistance (ESR) of components. This LCR meter can provide a 40,000 – count primary parameter reading and secondary parameter reading with a resolution of 0.0001 with an accuracy of up to 0.1%. we can use five particular test frequencies in this model such as: 100 Hz, 120 Hz, 1 kHz, 10 kHz, and 100 kHz. We can also select specific test voltage values from 0.3 V, 0.6 V, and 1 V.

With adjustable testing frequencies, voltage levels, and 4-probe measurements, the meter enables direct and reliable measurements in series or parallel modes. The auto range can quickly display the measurement findings and select the appropriate testing parameters based on the component qualities. This model can be accesses remotely by connecting it to a PC with mini-USB interface. Upon installation of a USB driver, the PC can control the instrument over virtual COM. Once the configurations are done, the LCR meter can be used in remote mode either by controlling the actions with standard command protocols using programming commands such as

IEEE 488 and Standard Commands for Programmable Instruments (SCPI). For ease-of-use BK precision also provides software named LCR Software from which one can select the parameters, acquire the readings and export them in either .txt or .xlsx format. You can also access the stored data from stand-alone measurements and transfer them to your PC.

It gives the option to acquire data either with 3 – terminal test port or 5 – terminal test port, in which 5 – terminal port gives more accurate measurements by using 4 – probe connection with a shield, which we are using to calculate the primary and secondary parameters for thin-film oxides of hafnium, zirconium, titanium etc.

Appendix C. Automated remote acquisition setup using Raspberry Pi 3 A+

It was proposed to design an acquisition system that can record the readings from the LCR meter without too much intervention of an operator and to access the recorded data remotely by anywhere. This would help us to design an independent system of acquisition that can be placed inside the glove box for much accurate measures of LCR. In order to achieve this, we are integrating a micro-computer called Raspberry Pi 3 A+, LCR meter is connected to the Pi which then can be accessed by anyone with the passcode to record and operate the LCR meter reading. A python file is created to program the LCR meter according to the user requirement and can be runed to acquire the values from the sample.

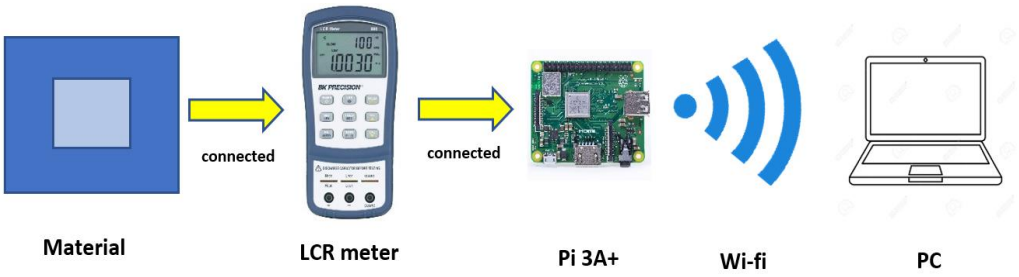


Figure 1. simple working schematic of the acquisition system

Appendix D. Relay-based switching in remote LCR acquisition application:

An 8 channel 5V relay board compatible with Raspberry pi 3A+ was used (figure 1) to electrically switch between samples in LCR remote acquisition process. One can use python to create a script that can automatically switch between samples after each set of acquisition. The data is locally stored inside Pi module which then can be used in analysis

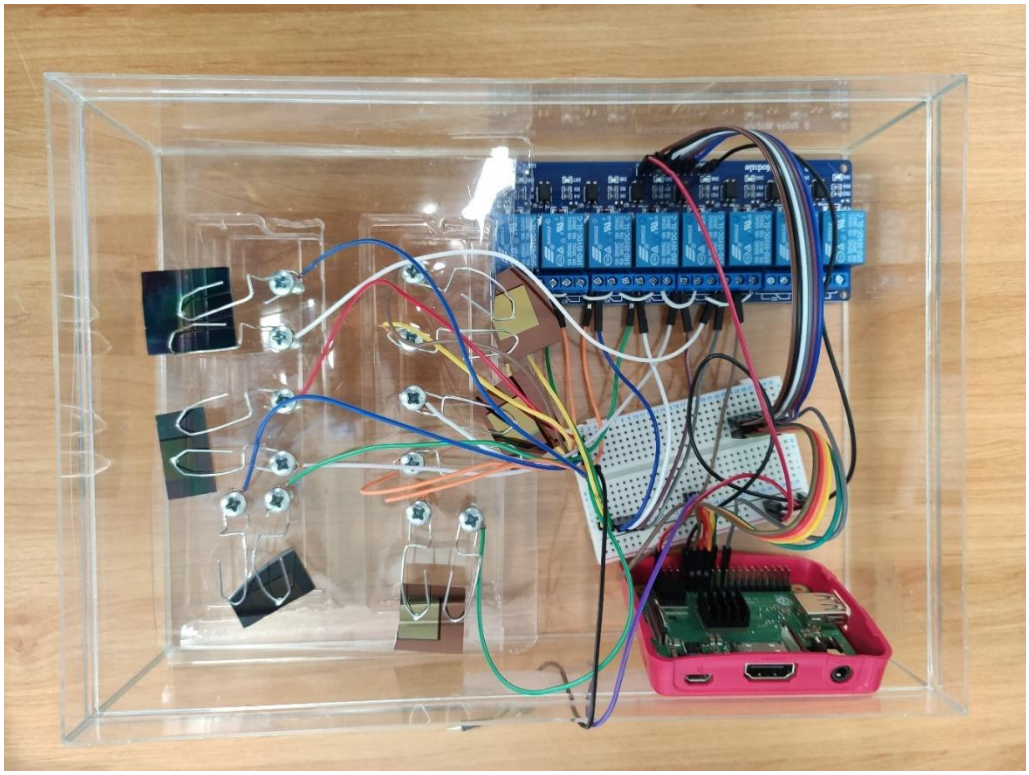


Figure1. Connection of relay module to Raspberry Pi and sample.